PROGRAMA DE TRABAJO AUDITORIA IDS

Objetivo: Verificar el correcto uso del Sistema de Detección de Intrusos de acuerdo a las políticas definidas en la Entidad.

Alcance:

1. Cobertura informática: automatización, análisis y evaluación de los controles establecidos para la detección de intrusos, y el tratamiento de incidencias.

2. Seguridad Lógica / Logs: análisis de la correcta definición de usuarios y perfiles con acceso al Sistema de Detección de Intrusos así como la parametrización de seguridad. verificar la existencia de procesos que permitan realizar el seguimiento de las operaciones críticas realizadas en el sistema.

3. Documentación: revisión de la documentación relacionada con el diseño y la explotación del Sistema de Detección de Intrusos.

4. Proveedores externos: verificación de los servicios y la documentación que da soporte a la relación contractual con los proveedores externos para determinar su adaptación a los requerimientos del BCRA.

5. Continuidad de Procesamiento y Backup: análisis y evaluación de los procedimientos establecidos para la realización de backups periódicos y recuperación de la información en situaciones de contingencia informática.

SEGU-INFO.COM.AR

1. Cobertura Informática

a. **Cobertura de Red** / Diagrama de red - Servidores:
- Verificar la existencia de un diagrama de red de la compañía.
- Obtener un diagrama de red de la compañía. Analizar que el mismo esta actualizado.
- Verificar la existencia de un diagrama de red detallando la ubicación del IDS.
- Obtener un diagrama de red detallando la ubicación del IDS. Analizar que el mismo esta actualizado. Analizar cual es la cobertura del IDS, que dirección IPs esta monitoreando.
- Verificar la existencia de una lista (o inventario) de los servidores de la compañía.
- Obtener un listado o inventario de los servidores de la compañía. Analizar si la misma esta actualizada. Obtener un detalle de los servidores que son considerados más críticos (vulnerables) y analizar si los mismos están siendo monitorizados por el IDS.

b. **Estrategia del IDS** / Tipo de IDS – Método implementado:
- Verificar el equipo incorporado. Analizar si el equipo implementado es IDS o IDS/IPS. Verificar si actualmente opera como IDS y/o IPS.
- Verificar el tipo de IDS implementado. Puede ser uno de los siguientes:
    1. IDS de Host.
    2. IDS de Red
    3. IDS Wireless
    4. IDS de análisis de comportamiento
- Verificar el método de análisis en que esta basado del IDS. Puede ser uno de los siguientes:
    1. Detección basada en firmas
    2. Detección basada en anomalías
    3. Detección basada en análisis de protocolos
- Verificar si todo el tráfico es analizado por el IDS. Obtener evidencia del tráfico que recibe el sensor para analizar. Obtener evidencia/detalle de la regla -*función span*- del switch que copia el tráfico al IDS) garantizando que no queda tráfico sin analizar.

c. **Configuración** / Configuración – Parametria:
- Verificar la correcta y adecuada configuración/parametrización del IDS.
- Analizar el tipo de tráfico que analizado y el tipo de tráfico que no analizado por el IDS (firmas, protocolos, paquetes,…)
- Analizar si el IDS posee una función para la administración remota y si la misma es utilizada. Quien la utiliza y la autorización correspondiente.
- Analizar si se puede importar y exportar los datos desde el motor de análisis. Detalles del circuito que envía los datos del sensor a la base de datos - ¿Qué pasa si se cae el servidor que contiene la base

SEGU-INFO.COM.AR

de datos? ¿El sensor continua con la recolección de datos y los envía a la base de datos cuando esta disponible nuevamente?
- Analizar si el IDS está configurado para reconocer las pautas y comportamiento de los usuarios? (Diferenciar entre trafico de red normal/habitual y anormal/inusual) (excepciones)
- Analizar si el IDS posee firmas para detectar código malicioso? (gusanos, troyanos…)
- Analizar si el IDS esta configurado para identificar IP spoofing. Caso contrario indagar sobre la existencia de otros mecanismos (router, firewall,…) que cubran este aspecto y su disponibilidad.
- Analizar si el IDS esta configurado para enviar alertas cuando ocurre una intrusión de alto nivel y minimizar las alertas resultantes de falsos positivos y ataques de bajo nivel.
- ¿Por qué medios emite las alertas el IDS? (por ejemplo: e-mail, páginas web…)
- Analizar si los mecanismos automatizados de respuesta están disponibles.
- Analizar si los filtros están definidos en base a las políticas de seguridad para minimizar los falsos positivos.
- Analizar si el IDS tiene la capacidad de analizar los protocolos de la capa de aplicación con suficiente detalle.

d. **Base de Datos** / Almacenamiento:
- Verificar la registración de los eventos monitoreados que son alojados en la base de datos del IDS.
- ¿Dónde se almacenan? (Equipo: nombre, ubicación física).
- ¿Cada cuanto se reciclan?
- ¿Cómo y quién accede a ellos?
- ¿Se realizan backups? ¿Con que frecuencia? ¿Durante cuanto tiempo?

e. Interacción con el Firewall - Router / Relación con el Firewall - Router:
- Verificar si la implementación del IDS / IPS conlleva una interacción con el Firewall.
- Analizar si la implementación del IDS ha requerido la instalación de software en el Firewall/ routers.
- Analizar si el sistema se comunica con firewalls / routers. ¿Es esta comunicación una línea segura?
- Analizar si el IDS indica acciones preventivas a tomar por el Firewall o Router (por ejemplo: cerrando puertos o bloqueando IPs).

f. **Firmas – Aspectos Técnicos** / Firmas – Aspectos Técnicos:
- Verificar que el sistema posee actualizaciones de las firmas que sirven para identificar código malicioso (gusanos, troyanos…).
- Analizar con que frecuencia se actualizan las firmas. ¿se realiza una confirmación de autenticación e integridad sobre la actualización de las firmas?
- ¿Las actualizaciones son distribuidas a través de un medio/método seguro? (como cifrados o firmas digitales)

SEGU-INFO.COM.AR

- ¿Quién realiza la tarea de actualizar las reglas/firmas del IDS?
- ¿La Información de los últimos ataques se utiliza para mantener actualizado el IDS?
- ¿El IDS es escalable? (¿muchos sensores pueden ser monitoreados y administrados a la vez?).
- ¿El producto tiene un bajo efecto/impacto sobre el rendimiento de la red/host?
- ¿El máximo ancho de banda del sistema se ha medido para realizar un análisis sin pérdida, de manera que proporciona un análisis de cobertura del 100 por ciento, siendo compatible con las necesidades de la organización?
- Si se genera una gran cantidad de alarmas, ¿Todas son capturadas y registradas en una base de datos?
- ¿Se utiliza el IDS como complemento de la actividad de administración de la red, por ejemplo: como la administración de dispositivos de red?
- ¿Se encuentra el IDS integrado con estudios de vulnerabilidad de otros productos?

g. **Disponibilidad** / Disponibilidad – Redundancia:
- Verificar y analizar el grado de disponibilidad que ofrece el equipo y el servicio del Sistema de Detección de Intrusos.
- ¿El IDS opera 7x24 los 365 días del año? ¿En que días y franjas horarias se atienden las alarmas que informa el IDS? ¿Siempre hay personal disponible? ¿Cuál es el circuito establecido para atender alarmas cuando no hay usuarios que se encuentren operando con el IDS en las instalaciones?
- Analizar si existe hardware redundante disponible tales como duplicar las fuentes de alimentación, tarjetas de red, dispositivos de almacenamiento (por ejemplo, discos duros, flash ROM), y CPUs.
- Analizar si existe redundancia de software en el producto, sobre todo para los sensores, como el de reiniciar automáticamente el producto.
- Si es un IPS: ¿Puede el producto administrar múltiples servidores de manera que si uno falla los sensores automáticamente no dejan sin atender a otros?
- Analizar si pueden haber desplegados múltiples sensores para observar la actividad de la misma manera en caso de que si uno falla, otro automáticamente asume sus responsabilidades.
- Si un sensor falla, ¿la facilidad de configuración puede ser trasladada a otros sensores (por ejemplo, la transferencia de una configuración del sensor en CD y disquetes de configuración desde el primer sensor para el segundo sensor, y luego reiniciarlo)?

h. **Capacitación** / Capacitación / Entrenamiento:
- Verificar si el personal que opera con el servicio ofrecido por el Sistema de Detección de Intrusos recibe capacitación para explotar el IDS de acuerdo a las políticas internas establecidas.

SEGU-INFO.COM.AR

- Analizar si se realiza capacitación al personal correspondiente con los conocimientos especializados para la configuración, mantenimiento y análisis de los resultados del IDS en forma periódica. ¿Cómo es la capacitación (Manuales, Cursos a Distancia, Cursos Presenciales,…)?
- Analizar si el personal que opera con el IDS interactúa con foros o comunidades que provean información para asistir en consultas e incidencias.

i. **Complemento - Mecanismos de Protección** / Mecanismos de Protección:
   - Verificar los mecanismos de protección, adicionales a la actividad del IDS, que existen para:
   - Algún usuario pueda conectarse desde la red interna a otra red en forma desautorizada utilizando un módem u otro dispositivo.
   - Algún usuario puede ejecutar software en la red LAN/WAN de forma desautorizada generando una amenaza de seguridad que comprometa a equipos de la red. (por ejemplo: Back Orifice)
   - Algún usuario pueda ejecutar programas del tipo P2P (peer to peer) los cuales son utilizados para el ingreso y egreso de información en forma desautorizada (por ejemplo: ares, kazaa, emule, bitorrent, edonkey, imesh, morpheus, shareaza, soolseek,…)
   - Algún usuario pueda ejecutar programas de mensajería instantánea o acceder a los mismos mediante una página web (por ejemplo: http://webmessenger.msn.com/)
   - Ingreso o salida de e-mails con información adjunta que contenga código malicioso a fin de que sean restringidos sin comprometer la productividad.
   - Direcciones parecidas con las URLs que pueden presentar una amenaza para la seguridad como algunos sitios web que están configurados para explotar una red mediante vulnerabilidades en los navegadores.
   - Hardening: (Fortalecimiento del Sistema Operativo):
     - Reportes con el estado de las actualizaciones realizadas en las estaciones de trabajo y servidores. Se debe verificar que poseen las actualizaciones con los parches de seguridad (Service Pack) actualizados a fin de mitigar el riesgo de las actividades que amenazan a los Sistemas Operativos aprovechando las vulnerabilidades de su diseño.
   - Antivirus:
     - Antivirus web (on line): detalles del antivirus, frecuencia de actualización, disponibilidad en que opera, alcance de la red (en que equipos opera)
     - Antivirus de escritorio: detalles del antivirus, frecuencia de actualización, disponibilidad en que opera, alcance de la red (en que equipos opera).
   - Honeypots / Honeynets:

SEGU-INFO.COM.AR

- Verificar la existencia de Honeypots o Honeynet en la compañía.
- Analizar si se ha implementado una Honeypot Hibrida.
- Honeypot:
  - Analizar el tipo de Honeypot
    - De Producción
    - De Investigación
  - Analizar el tipo de clasificación del servicio del Honeypot
    - De Compromiso Bajo
    - De Compromiso Medio
    - De Compromiso Alto
  - Analizar su ubicación en la red
    - Antes del Firewall
    - Después del Firewall
    - En la DMZ
  - Analizar la relación del IDS/IPS con el Honeypot.
  - Analizar la administración del Honeypot
  - Analizar la actividad registrada
  - Analizar los reportes, informes emitidos
  - Obtener detalles, reportes de casos detectados sobre ataques intrusiones si los hubo y las acciones tomadas.
- Honeynet:
  - Analizar la relación del IDS/IPS con el Honeynet.
  - Analizar si se ha implementado una Honeynet virtual.
  - Analizar si se ha implementado una Honeynet Distribuida.
  - Analizar que tipo de Generación de Honeynet esta implementada (Generación 1 o 2)
  - Analizar la administración de la Honeynet
  - Analizar la actividad registrada
  - Analizar los reportes, informes emitidos
  - Obtener detalles, reportes de casos detectados sobre ataques intrusiones si los hubo y las acciones tomadas.

SEGU-INFO.COM.AR

2. Seguridad Lógica / Logs

a. **Usuarios** / Usuarios:
   - Verificar que los usuarios que operan con el IDS pertenecen a la nomina de la compañía.
   - Analizar los usuarios que operan con el IDS y chequear que pertenecen a la nomina de la compañía como personal efectivo y/o contratado.

b. **Perfiles** / Perfiles:
   - Verificar que los usuarios que operan con el IDS poseen el perfil correspondiente de acuerdo a lo definido por el área de Organización.
   - Analizar el perfil de los usuarios (administradores, operadores) que operan con el servicio que brinda el IDS (consola, reporting) y chequear que el perfil asignado corresponde con las definiciones establecidas por el área de Organización.

c. **Accesos** / Accesos:
   - Verificar que los usuarios que operan con el IDS son los únicos autorizados a acceder a la información que brinda el Sistema de Detección de Intrusos, tanto en la base de datos, como la consola y repositorios donde se puedan alojar reportes o informes (logs) de la actividad monitoreada.
   - Analizar los accesos al equipo IDS, al servidor que contiene la base de datos alimentada por el IDS y (si existe) rutas o equipos donde se alojen informes o reportes (logs) del IDS sobre la actividad monitoreada.

SEGU-INFO.COM.AR

3. Documentación

a. **Reportes /** Reportes del IDS:
   - Verificar la eficiencia y eficacia de los reportes suministrados por el IDS.
   - Analizar la existencia de reportes de casos detectados que llevaron a tomar acciones de prevención (por ejemplo: bloquear un rango de IPs para evitar el inicio de un ataque o la prolongación del mismo)
   - Obtener una lista de falsos positivos emitidos por el IDS.
   - Obtener reportes con estadísticas de los eventos detectados.
   - Analizar la existencia de un modulo de reporte para definir ataques determinados en un periodo dado. (Por ejemplo, por hora, semana, mes…).

b. **Manual de usuario /** Manual de Usuario del IDS:
   - Verificar la existencia de un manual del usuario del IDS.
   - Analizar si el mismo esta actualizado.

c. **Normativa Interna /** Normas y Políticas:
   - Política de seguridad: la misma presenta una declaración de intenciones y objetivos de la organización respecto a sus necesidades de seguridad y establece qué seguridad se necesita y por qué.
   - Verificar la existencia de Normativa Interna y/o Políticas de Seguridad sobre comportamiento interno o externo que comprometa a la red o el funcionamiento normal / habitual del negocio.
   - Analizar la documentación correspondiente si la misma indica como responder a los ataques de red la cual debería incluir la preparación, detección, contención, erradicación, recuperación y seguimiento.
   - Analizar la existencia de un procedimiento detallado que exprese las medidas que deben adoptarse cuando el IDS detecta un problema.
   - Analizar la existencia de un procedimiento que indica acciones disciplinarias que se toman cuando se encuentran empleados que espían/monitorean (snooping) la red y ejecutan software de hacking.
   - Analizar la existencia de normativa interna sobre el uso de software legal, antivirus, seguridad en Internet y protección contra software malicioso.
   - Analizar si la política implica mecanismos de una administración de seguridad sobre los recursos de la Entidad en los siguientes aspectos:
     - Separación de funciones
     - Rotación del trabajo
     - Menor privilegio

SEGU-INFO.COM.AR

  - Necesidad de saber
  - Vacaciones obligadas
- Analizar si la política de Seguridad presenta una declaración expresa sobre la prohibición del uso de software del tipo:
  - Software de mensajería instantánea (puede ser mediante la ejecución de programas o páginas web)
  - Software P2P (peer-to-peer)

d. **Diagramas** / Diagramas de flujo – Procesos:
   - Verificar la existencia de un diagrama de flujo/proceso que exprese el circuito del IDS cuando se emiten alertas notificando a los sectores involucrados de tomar las acciones correspondientes y definidas por la política de la compañía.

e. **Plan de Seguridad** / Plan de Seguridad:
   - Plan de seguridad: siendo que el mismo presenta una secuencia de proyectos de implantación de medidas para poder satisfacer las necesidades de seguridad y el mismo indica la ejecución de acciones para lograr el cumplimiento de la política debe contener mínimamente el establecimiento de plazos, recursos, acciones,… etc.
   - Verificar la existencia de un plan de Seguridad y que abarque los proyectos actuales y futuros. (Sea en corto, mediano o largo plazo).
   - Analizar que el plan de Seguridad esta alineado con la política de Seguridad.
   - Analizar si el plan de Seguridad posee proyectos para modificar la implementación del IDS y como está establecido el mismo. También debiera incluir un plan de concientización (awareness) al personal de la compañía sobre los recursos de la organización y correcto uso de los mismos de acuerdo a la necesidad de conocer y las políticas de la Empresa.

f. **Actas** / Actas de Registración
   - Verificar la existencia de actas de registración donde se expresan los eventos detectados y acciones de carácter excepcional.
   - Analizar si el acta registra los siguientes eventos:
     1. Uso de claves sensitivas.
     2. Detección de intrusión.
     3. Caídas de servicios (por fallas de software y/o hardware).
     4. Uso inapropiados de privilegios.
     5. Solicitudes excepcionales.

SEGU-INFO.COM.AR

4. Proveedores Externos

a. **Proveedores** / Proveedores externos:
   - Verificar si un proveedor externo ofrece algún tipo de servicio vinculado sobre el Sistema de Detección de Intrusos (Consultaría, capacitación, test de penetración/vulnerabilidades)
   - Verificar si existe un proveedor que proporcione información y ayuda en la respuesta a incidentes.
   - Verificar si existe un proveedor que proporcione Soporte Técnico sobre el equipo IDS.
   - Verificar y analizar el contrato establecido entre el proveedor externo y la compañía cubriendo aspectos tales como: vigencia, disponibilidad y confidencialidad.
   - Si un proveedor realiza test de penetración:
     a. Verificar la existencia de un contrato establecido entre la compañía y el proveedor externo cubriendo aspectos tales como: objetivo, alcance, plazos del servicio, vigencia, confidencialidad e informes detallando los resultados y las recomendaciones del test realizado.
     b. Obtener una muestra de reportes/informes de test realizados.

SEGU-INFO.COM.AR

5. Continuidad de Procesamiento

a. **Backups /** Backups – Almacenamiento:
   - Verificar el adecuado respaldo de la actividad registrada por el IDS.
   - Verificar la registración de los eventos monitoreados que son alojados en la base de datos del IDS.
   - ¿Dónde se almacenan? (Equipo: nombre, ubicación física).
   - ¿Cada cuanto se reciclan?
   - ¿Cómo y quién accede a ellos?
   - ¿Se realizan backups? ¿Con que frecuencia? ¿Durante cuanto tiempo? ¿Cuántas copias se realizan y donde se alojan?
   - Verificar que es posible realizar un recupero de la actividad almacenada en los backups.

SEGU-INFO.COM.AR

ANEXO

Referencias / Definiciones:

Documentación:

La política de seguridad debe implicar mecanismos de una administración de seguridad sobre los recursos de la Entidad en los siguientes aspectos:

1. Separación de funciones
2. Rotación del trabajo
3. Menor privilegio
4. Necesidad de saber
5. Vacaciones obligadas

1. Separación de funciones:
   a. Permite asegurar que una única persona no puede comprometer la seguridad de la empresa.
   b. Las funciones más importantes de una organización deberían estar separadas y distribuidas en diferentes individuos para su ejecución.
   c. Ayuda a prevenir errores que pueden tener lugar si una única persona cumple una función o tarea desde su comienzo hasta su fin.
2. Rotación del trabajo:
   a. Significa que más de una persona conoce las tareas de una determinada función dentro de la empresa.
   b. Esto permite contar con más de un individuo en capacidad de conocer las tareas y responsabilidades propias de una función o posición.
   c. Permite ayudar a identificar actividades fraudulentas, por lo que puede considerarse como un "Control Detectivo".
   d. Brinda la oportunidad de disponer de un "backup" en caso que el responsable de la función deje la empresa o se encuentre ausente.
3. Menor privilegio:
   a. Significa que un individuo dentro de la organización debe tener sólo los derechos y permisos necesarios para el cumplimiento de sus funciones.
   b. Si un empleado tuviera excesivos derechos y permisos podría abusar de los mismos, poniendo en riesgo a la organización.
4. Necesidad de saber:
   a. Este principio se encuentra en estrecha relación con el de "Menor Privilegio".
   b. Cada usuario de la organización debería tener "Necesidad de saber" sólo aquella información requerida para el cumplimiento de sus funciones.
   c. Siguiendo este principio, un usuario sólo debería acceder a aquellos recursos que le están permitidos
5. Vacaciones Obligadas:
   a. Permite la implementación del principio de "Rotación del trabajo".
   b. Puede detectar actividades fraudulentas.

SEGU-INFO.COM.AR

Diccionario

ACTIVO:

Cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la compañía.

ACTIVISMO / HACKTIVISMO:

Se entiende normalmente la escritura de código o la manipulación de bits para promover una ideología política, generalmente promoviendo políticas tales como la libertad de expresión, derechos humanos y ética de la información. El término fue acuñado por el crítico cultural y autor Jason Sack en un artículo sobre el artista de medios Shi Lea Cheang y publicado en InfoNation en 1995. Los actos del hacktivismo se llevan a cabo por personas que consideran que el uso apropiado el código puede tener efectos similares al activismo corriente o a la desobediencia civil. Pocas personas pueden escribir código, pero afecta a más personas.

ADMINISTRADOR, sysop, root:

Es la persona que se encarga del sistema. Se suele denominar "root" y es la persona que tiene el poder absoluto sobre la maquina/sistema.

AGUJERO, bug, hole:

Es un efecto en el software o hardware que como su nombre indica deja son fallas en el sistema, en otras palabras defectos de programación, o un defecto físico de un hardware.

AIX:
Sistema operativo de IBM.

ALERTA:

Notificación formal de que se ha producido un incidente relacionado con la seguridad de la información que puede evolucionar hasta convertirse en desastre.

ANONIMATO:

Condición en la que la verdadera identidad de un individuo es desconocida.

ARP:

ARP son las siglas en inglés de Address Resolution Protocol (Protocolo de resolución de direcciones). Es un protocolo de nivel de red responsable de encontrar la dirección hardware (Ethernet MAC) que corresponde a una determinada dirección IP. Para ello se envía un paquete (ARP request) a la dirección de multidifusión de la red (broadcast (MAC = ff ff ff ff ff ff)) conteniendo la dirección IP por la que se pregunta, y se espera a que esa máquina (u otra) responda (ARP reply) con la dirección Ethernet que le corresponde. Cada máquina mantiene una caché con las direcciones traducidas para reducir el retardo y la carga. ARP permite a la dirección de Internet ser independiente de la dirección Ethernet, pero esto solo funciona si todas las máquinas lo soportan.

ARP está documentado en el RFC (Request For Comments) 826.

El protocolo RARP realiza la operación inversa.

En Ethernet, la capa de enlace trabaja con direcciones físicas. El protocolo ARP se encarga de traducir las direcciones IP a direcciones MAC (direcciones físicas).Para realizar

SEGU-INFO.COM.AR

ésta conversión, el nivel de enlace utiliza las tablas ARP, cada interfaz tiene tanto una dirección IP como una dirección física MAC.

ARP se utiliza en 4 casos referentes a la comunicación entre 2 hosts:

Cuando 2 hosts están en la misma red y uno quiere enviar un paquete a otro.

Cuando 2 host están sobre redes diferentes y deben usar un gateway/router para alcanzar otro host.

Cuando un router necesita enviar un paquete a un host a través de otro router.

Cuando un router necesita enviar un paquete a un host de la misma red.

Tabla de contenidos

Tablas ARP:

La filosofía es la misma que tendríamos para localizar al señor X entre 150 personas: preguntar por su nombre a todo el mundo, y el señor X nos responderá. Así, cuando a A le llegue un mensaje con dirección origen IP y no tenga esa dirección en su tabla ARP, enviará su frame ARP a la dirección broadcast (física), con la IP de la que quiere conocer su dirección física. Entonces, el equipo cuya dirección IP coincida con la preguntada, responderá a A enviándole su dirección física. En este momento A ya puede agregar la entrada de esa IP a su tabla ARP. Las entradas de la tabla se borran cada cierto tiempo, ya que las direcciones físicas de la red pueden cambiar (Ej: si se estropea una tarjeta de red y hay que sustituirla)

Funcionamiento I

Si A quiere enviar un frame a la dirección IP de B (misma red), mirará su tabla ARP para poner en la frame la dirección destino física correspondiente a la IP de B. De esta forma, cuando les llegue a todos el frame, no tendrán que deshacer el frame para comprobar si el mensaje es para ellos, sino que se hace con la dirección física.

Funcionamiento II

Si A quiere enviar un mensaje a C (un nodo que no este en la misma red), el mensaje deberá salir de la red. Así, A envía el frame a la dirección física del router de salida. Esta dirección física la obtendrá a partir de la IP del router, utilizando la tabla ARP. Si esta entrada no esta en la tabla, mandará un mensaje ARP a esa IP (llegará a todos), para que le conteste indicándole su dirección física.

Ejemplo Address Resolution Protocol Una vez en el router, éste consultará su tabla de encaminamiento, obteniendo el próximo nodo (salto) para llegar al destino, y saca el mensaje por el interfaz correspondiente. Esto se repite por todos los nodos, hasta llegar al último router, que es el que comparte el medio con el host destino. Aquí el proceso cambia: el interfaz del router tendrá que averiguar la dirección física de la IP destino que le ha llegado. Lo hace mirando su tabla ARP o preguntando a todos.

AUTENTICACIÓN:

Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

AWARENESS TRAINIG:

SEGU-INFO.COM.AR

Proceso a través del cual:

- Los usuarios reconocen la importancia de la seguridad de la información y los activos de la información.
- Se preocupan en forma proactiva por la misma
- Responden de manera adecuada ante cualquier evento o circunstancia.

AXIOMA:

Sentencia que no necesita demostración alguna por su evidencia.

BACKDOOR:
Puerta trasera. Mecanismo que tiene o que se debe crear en un software para acceder de manera no autorizada.

BBS (Bulletin Board System):

Es una maquina a la que se accede a través de la línea telefónica y donde se dejan mensajes y software.

BCP: (Business Continuity Plan)

Plan orientado a permitir la continuación de las principales funciones del negocio de la compañía en el caso de imprevisto que atente contra el mismo.

BOMBA DE CORREO:

Es una cantidad excesiva de información en correo electrónico enviada a la dirección de un usuario en un intento por hacer que el programa de correo electrónico del usuario colapse.

BOMBA LOGICA:

Código que ejecuta una particular manera de ataque cuando una determinada condición se produce. Por ejemplo una bomba lógica puede formatear el disco rígido un día y hora determinado/a

BOXING:
Uso de aparatos electrónicos o eléctricos (Boxes) para hacer phreaking. Esto no es hacking sino phreaking

BOUNCER:
Técnica que consiste en usar una maquina de puente y que consigue que haciendo un telnet al puerto xxxx, ésta redirecciona la salida a un puerto determinado de otra maquina. Esta técnica es muy usada en el irc redireccionando a los puertos destinados a los servidores de irc, en otras palabras, buscando ser anónimo.

BRIDGE:

Un puente o bridge es un dispositivo de interconexión de redes de ordenadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Este interconecta dos segmentos de red (o divide una red en segmentos) haciendo el pasaje de datos de una red para otra, con base en la dirección física de destino de cada paquete.

Un bridge conecta dos redes como una sola red usando el mismo protocolo de establecimiento de red.

Funciona a través de una tabla de direcciones MAC detectadas en cada segmento a que esta conectado. Cuando detecta que un nodo de uno de los segmentos está intentando transmitir

SEGU-INFO.COM.AR

datos a un nodo del otro, el bridge copia la trama para la otra subred. Por utilizar este mecanismo de aprendizaje automático, los bridges no necesitan configuración manual.

Ejemplo de 2 redes interconectadas por un bridge.

La principal diferencia entre un bridge y un hub es que el segundo pasa cualquier trama con cualquier destino para todos los otros nodos conectados, en cambio el primer sólo pasa las tramas pertenecientes a cada segmento. Esta característica mejora el rendimiento de las redes al disminuir el tráfico inútil.

BRUTE FORCE O FUERZA BRUTA:

Es el procedimiento que usan tanto los crackeadores de password de UNIX como los de NT, se basan en aprovechar diccionarios para obtener los passwords del un sistema.

CALIFICACIÓN DEL DELITO:

En el procedimiento criminal, motiva el escrito de calificación o conclusiones que el ministerio fiscal, el abogado querellante y la defensa formula al ser elevada la causa a plenario.

CIFRADO:

Algoritmo que permite codificar los datos mediante claves para que resulte un código equivalente pero ininteligible, de forma que solo quienes conozcan la clave puedan acceder al contenido real de los datos.

CLOACKER:
Programa que borra los logs (huellas) en un sistema. También llamados zappers.

CODIGO CIVIL:

Texto legal que contienen lo referente sobre el régimen jurídico, aplicable a personas, bienes, sucesiones, obligaciones y contratos.

CODIGO PENAL:

Texto legal que define los delitos y las faltas, sus correspondientes penas y las responsabilidades de ellas.

CODIGO MALICIOSO:

Software capaz de realizar un proceso no autorizado sobre un sistema con un deliberado propósito de ser perjudicial. Virus, gusanos, troyanos son algunos ejemplos de código malintencionado.

CONFIDENCIALIDAD:

Se refiere al acceso a la información por parte únicamente de quienes estén autorizados.

CONTROL:

Conjunto de políticas, procedimientos, prácticas y estructuras organizativas que aseguran una garantía razonable o suficiente de que se lograran los objetivos de negocio y/o se corregirán de ser necesario.

CRACKEADOR DE PASSWORDS:

SEGU-INFO.COM.AR

Programa utilizado para sacar los password encriptados de los archivos de passwords.

CRACKER:

El término cracker (del inglés crack, romper) tiene varias acepciones. En conclusión se roba información. Es como el ladrón en un robo.

Cracker es una persona que mediante ingeniería inversa realiza: seriales, keygens y cracks.

Un cracker es alguien que viola la seguridad de un sistema informático de forma similar a como lo haría un hacker, sólo que a diferencia de este último, el cracker realiza la intrusión con fines de beneficio personal o para hacer daño.

El término deriva de la expresión "criminal hacker", y fue creado alrededor de 1985 por contraposición al término hacker, en defensa de éstos últimos por el uso incorrecto del término.

Se considera que la actividad de esta clase de cracker es dañina e ilegal.

También se denomina cracker a quien diseña o programa cracks informáticos, que sirven para modificar el comportamiento o ampliar la funcionalidad del software o hardware original al que se aplican, sin que en absoluto pretenda ser dañino para el usuario del mismo.

No puede considerarse que la actividad de esta clase de cracker sea ilegal si ha obtenido el software o hardware legítimamente, aunque la distribución de los cracks pudiera serlo.

Asimismo, un cracker también es aquel que practica el cracking (acción de modificar el código fuente a un programa). Ésta actividad está prohibida a menos que el programa al que se le aplica sea de Software libre, y por lo general requiere muchos conocimientos sobre hacking.

DAEMON:

Proceso en background en los sistemas Unix, es decir un proceso que esta ejecutándose en segundo plano.

DATA DIDDLING:

Esta categoría se refiere a la modificación desautorizada a los datos, o al software instalado en un sistema, incluyendo borrado de archivos. Este tipo de ataques son particularmente serios cuando el que lo realiza ha obtenido derechos de administrador o supervisor, con la capacidad de disparar cualquier comando y por ende alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema en forma deliverada. O aún si no hubo intenciones de ello, el administrador posiblemente necesite dar de baja por horas o días hasta chequear y tratar de recuperar aquella información que ha sido alterada o borrada.

Como siempre, esto puede ser realizado por insiders u outsiders, generalmente con el propósito de fraude o dejar fuera de servicio un competidor.

DELITO:

Acciones y omisiones dolosas y culpables penadas por la ley.

DELITO CULPOSO:

Aquel en que esta ausente del dolo, se comete por imprudencia o negligencia.

DELITO POR OMISION:

Consiste en la omisión de un deber, siendo la infracción cometida por no cumplir lo mandado.

DELITO DOLOSO:

SEGU-INFO.COM.AR

Delito cometido con conciencia y voluntad.

DENEGACION DE SERVICIO:

Se refiere a cuando una computadora o un programa dejan de responder al servicio solicitado por un saturamiento en la cantidad de solicitudes realizadas de forma maliciosa.

DESASTRE:

Evento natural, accidental o intencional que amenaza o interrumpe la operación habitual durante el tiempo suficiente para afectar de manera significativa al negocio.

DHCP:

DHCP son las siglas en inglés de Protocolo de configuración dinámica de servidores (Dynamic Host Configuration Protocol). Es un protocolo de red en el que un servidor provee los parámetros de configuración a las computadoras conectadas a la red informática que los requieran (máscara, puerta de enlace y otros) y también incluye un mecanismo de asignación de direcciones de IP. Este protocolo apareció como un protocolo estándar en octubre de 1993. En RFC 2131 (Inglés) se puede encontrar la definición más actualizada. Los últimos esfuerzos describiendo DHCPv6, DHCP en una red IPv6, fue publicado como RFC 3315 (Inglés)

DISPONIBILIDAD:

Propiedad que requiere que los recursos de un sistema abierto sean accesibles y utilizables a petición de una entidad autorizada.

DIVULGACION:

Es un componente del principio de aviso, por el cual una compañía debe poner a disposición sus practicas de manejo de información, incluyendo avisos de cómo reúne, utiliza y comparte información.

DOLO:

Engaño y fraude. Voluntad deliberada de cometer un delito a sabiendas a su ilicitud.

DNS:

El Domain Name System (DNS) es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar distintos tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio. La asignación de nombres a direcciones IP es ciertamente la función más conocida de los protocolos DNS. Por ejemplo, si la dirección IP del sitio FTP de prox.ve es 200.64.128.4, la mayoría de la gente llega a este equipo especificando ftp.prox.ve y no la dirección IP. Además de ser más fácil de recordar, el nombre es más fiable. La dirección numérica podría cambiar por muchas razones, sin que tenga que cambiar el nombre. Inicialmente, el DNS nació de la necesidad de recordar fácilmente los nombres de todos los servidores conectados a Internet. En un inicio, SRI (ahora SRI International) alojaba un archivo llamado HOSTS que contenía todos los nombres de dominio conocidos (técnicamente, este archivo aún existe - la mayoría de los sistemas operativos actuales todavía pueden ser configurados para revisar su archivo hosts). El crecimiento explosivo de la red causó que el sistema de nombres centralizado en el archivo HOSTS no resultara práctico y en 1983, Paul Mockapetris publicó los RFCs 882 y 883 definiendo lo que hoy en día ha evolucionado al DNS moderno. (Estos RFCs han quedado obsoletos por la publicación en 1987 de los RFCs 1034 y 1035).

SEGU-INFO.COM.AR

DOS (DDOS):

En seguridad informática, un ataque de denegación de servicio, también llamado ataque DoS (de las siglas en inglés Denial of Service), es un ataque a un sistema de ordenadores o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima. Se genera mediante la saturación de los puertos con flujo de información, haciendo que el servidor se sobrecargue y no pueda seguir prestando servicios, por eso se le dice "denegación", pues hace que el servidor no de abasto a la cantidad de usuarios. Esta técnica es usada por los llamados crackers para dejar fuera de servicio a servidores objetivo. El llamado DDoS (siglas en inglés de Distributed Denial of Service, denegación de servicio distribuida) es una ampliación del ataque DoS, se efectúa con la instalación de varios agentes remotos en muchas computadoras que pueden estar localizadas en diferentes puntos. El invasor consigue coordinar esos agentes para así, de forma masiva, amplificar el volumen del flood o saturación de información, pudiendo darse casos de un ataque de cientos o millares de computadoras dirigido a una máquina o red objetivo. Esta técnica se ha revelado como una de las más eficaces y sencillas a la hora de colapsar servidores, la tecnología distribuida ha ido sofisticándose hasta el punto de otorgar poder de causar daños serios a personas con escaso conocimiento técnico. En ocasiones, esta herramienta ha sido utilizada como un notable método para comprobar la capacidad de tráfico que un ordenador puede soportar sin volverse inestable y perjudicar los servicios que desempeña. Un administrador de redes puede así conocer la capacidad real de cada máquina.

EAVESDROPPING:

La interceptación o eavesdropping, también conocida por passive wiretapping es un proceso mediante el cual un agente capta información - en claro o cifrada - que no le iba dirigida; esta captación puede realizarse por muchísimos medios (por ejemplo, capturando las radiaciones electromagnéticas). Aunque es en principio un ataque completamente pasivo, lo más peligroso del eavesdropping es que es muy difícil de detectar mientras que se produce, de forma que un atacante puede capturar información privilegiada y claves para acceder a más información sin que nadie se de cuenta hasta que dicho atacante utiliza la información capturada, convirtiendo el ataque en activo.

EAVESDROPPING Y PACKET SNIFFING:

Muchas redes son vulnerables al eavesdropping, o la pasiva intercepción (sin modificación) del tráfico de red. En Internet esto es realizado por packet sniffers, que son programas que monitorean los paquetes de red que están direccionados a la computadora donde están instalados. El sniffer puede ser colocado tanto en una estación de trabajo conectada a red, como a un equipo router o a un gateway de Internet, y esto puede ser realizado por un usuario con legítimo acceso, o por un intruso que ha ingresado por otras vías. Existen kits disponibles para facilitar su instalación.

Este método es muy utilizado para capturar loginIDs y passwords de usuarios, que generalmente viajan claros (sin encriptar) al ingresar a sistemas de acceso remoto (RAS). También son utilizados para capturar números de tarjetas de crédito y direcciones de e-mailes entrantes y salientes. El análisis de tráfico puede ser utilizado también para determinar relaciones entre organizaciones e individuos.

ELEVACION DE PRIVILEGIOS:

Proceso mediante el cual el usuario engaña al sistema para que le otoru8e derechos no autorizados usualmente con el propósito de comprometer o destruir el sistema.

ENCRIPTACIÓN:

SEGU-INFO.COM.AR

Encriptación es el proceso mediante el cual cierta información o "texto plano" es cifrado de forma que el resultado sea ilegible a menos que se conozcan los datos necesarios para su interpretación. Es una medida de seguridad utilizada para que al momento de almacenar o transmitir información sensible ésta no pueda ser obtenida con facilidad por terceros. Opcionalmente puede existir además un proceso de desencriptación a través del cuál la información puede ser interpretada de nuevo a su estado original, aunque existen métodos de encriptación que no pueden ser revertidos.

Algunos de los usos más comunes de la encriptación son el almacenamiento y transmisión de información sensible como contraseñas, números de identificación legal, números de tarjetas de crédito, reportes administrativo-contables y conversaciones privadas, entre otros. La encriptación hace uso de diversas fórmulas matemáticas con el propósito de transformar el texto plano en un criptograma el cual es un conjunto de caracteres que a simple vista no tiene ningún sentido para el lector. La mayoría de los métodos de encriptación utilizan una clave como parámetro variable en las mencionadas fórmulas matemáticas de forma que a pesar de que un intruso las conozca, no le sea posible descifrar el criptograma si no conoce la clave, la cual solo se encuentra en posesión de las personas que pueden tener acceso a la información en cuestión. Algunos métodos utilizan incluso dos claves, una privada que se utiliza para la encriptación y otra pública para la desencriptación. En algunos métodos la clave pública no puede efectuar la desencriptación o descifrado, sino solamente comprobar que el criptograma fue encriptado o cifrado usando la clave privada correspondiente y no ha sido alterado o modificado desde entonces. La encriptación como proceso forma parte de la criptología, ciencia que estudia los sistemas utilizados para ocultar la información. Aunque la criptología surgió con gran anterioridad, la informática ha revolucionado los métodos que se utilizan para la encriptación/desencriptación de información, debido a la velocidad con que las computadoras pueden realizar las fórmulas matemáticas requeridas para llevar a cabo estos métodos y a la complejidad que han alcanzado debido a este hecho.

EXPLOITS:
Es un programa que aprovecha una vulnerabilidad (por código o diseño) para ingresar en un sistema

FALTA:

Acción u omisión voluntaria penada pro la ley con penas leves.

FAKE MAIL:

Enviar correo falseando el remitente. Se usa mucho en ingeniería social.

FALLO DE SEGURIDAD:

Programa o técnica que aprovecha una vulnerabilidad del software. Los fallos de seguridad pueden utilizarse para provocar brechas de seguridad o atacar un host en red por otros medios.

FIREWALL o Cortafuego:

Un cortafuegos (o firewall en inglés), es un elemento de hardware o software utilizado en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red que haya definido la organización responsable de la red. Su modo de funcionar es indicado por la recomendación RFC 2979, que define las características de comportamiento y requerimientos de interoperabilidad. La ubicación habitual de un cortafuegos es el punto de conexión de la red interna de la organización con la red exterior, que normalmente es Internet; de este modo se protege la red interna de intentos de acceso no autorizados desde Internet, que puedan aprovechar vulnerabilidades de los sistemas de la red interna.

SEGU-INFO.COM.AR

También es frecuente conectar al cortafuegos una tercera red, llamada zona desmilitarizada o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

Un cortafuegos correctamente configurado añade protección a una instalación informática, pero en ningún caso debe considerarse como suficiente. La Seguridad informática abarca más ámbitos y más niveles de trabajo y protección.

FIRMA DIGITAL: (Firma electrónica)

La firma digital es, en la transmisión de mensajes telemáticos, un método criptográfico que asegura su integridad así como la identidad del remitente.

Garantiza: Integridad, Autenticación y No repudio.

Contenidos:

La teoría

La firma digital de un documento es el resultado de aplicar cierto algoritmo matemático, denominado función hash, al contenido. Esta función asocia un valor dentro de un conjunto finito (generalmente los números naturales) a su entrada. Cuando la entrada es un documento, el resultado de la función es un número que identifica casi unívocamente al texto. Si se adjunta este número al texto, el destinatario puede aplicar de nuevo la función y comprobar su resultado con el que ha recibido. No obstante esto presenta algunas dificultades.

Las posibilidades de red

Para que sea de utilidad, la función hash debe satisfacer dos importantes requisitos. Primero, debe ser difícil encontrar dos documentos cuyo valor para la función "hash" sea idéntico. Segundo, dado uno de estos valores, debería ser difícil recuperar el documento que lo produjo.

Algunos sistemas de cifrado de clave pública se pueden usar para firmar documentos. El firmante cifra el documento con su clave privada y cualquiera que quiera comprobar la firma y ver el documento, no tiene más que usar la clave pública del firmante para descifrarla.

Existen funciones "hash" específicamente designadas para satisfacer estas dos importantes propiedades. SHA y MD5 son dos ejemplos de este tipo de algoritmos. Para usarlos un documento se firma con una función "hash", cuyo resultado es la firma. Otra persona puede comprobar la firma aplicando la misma función a su copia del documento y comparando el resultado con el del documento original. Si concuerdan, es casi seguro que los documentos son idénticos.

Claro que el problema está en usar una función "hash" para firmas digitales que no permita que un "atacante" interfiera en la comprobación de la firma. Si el documento y la firma se enviaran descifrados, este individuo podría modificar el documento y generar una firma correspondiente sin que lo supiera el destinatario. Si sólo se cifrara el documento, un atacante podría manipular la firma y hacer que la comprobación de ésta fallara. Una tercera opción es usar un sistema de cifrado híbrido para cifrar tanto la firma como el documento. El firmante usa su clave privada, y cualquiera puede usar su clave pública para comprobar la firma y el documento. Esto suena bien, pero en realidad no tiene sentido. Si este algoritmo hiciera el documento seguro también lo aseguraría de manipulaciones, y no habría necesidad

SEGU-INFO.COM.AR

de firmarlo. El problema más serio es que esto no protege de manipulaciones ni a la firma, ni al documento. Con este método, sólo la clave de sesión del sistema de cifrado simétrico es cifrada usando la clave privada del firmante. Cualquiera puede usar la clave pública y recuperar la clave de sesión. Por lo tanto, resulta obvio usarla para cifrar documentos substitutos y firmas para enviarlas a terceros en nombre del remitente.

La solución

Un algoritmo efectivo debe hacer uso de un sistema de clave pública para cifrar sólo la firma. En particular, el valor "hash" se cifra mediante el uso de la clave privada del firmante, de modo que cualquiera pueda comprobar la firma usando la clave pública correspondiente. El documento firmado se puede enviar usando cualquier otro algoritmo de cifrado, o incluso ninguno si es un documento público. Si el documento se modifica, la comprobación de la firma fallará, pero esto es precisamente lo que la verificación se supone que debe descubrir.

El Digital Signature Algorithm es un algoritmo de firmado de clave pública que funciona como hemos descrito. DSA es el algoritmo principal de firmado que se usa en GnuPG

Aplicaciones

Mensajes con autencididad asegurada

Contratos comerciales electrónicos

Factura _ electrónica

Desmaterialización de documentos

Transacciones comerciales electrónicas

Invitación electrónica

Dinero electrónico

Notificaciones judiciales electrónicas

Voto electrónico

Decretos ejecutivos (gobierno)

Créditos de seguridad social

Contratación pública

Sellado de tiempo

FONING:

Son personas con conocimientos en teléfonos modulares (TM) como en teléfonos móviles, se encuentran sumergidos en entendimientos de telecomunicaciones bastante amplios. Por lo general trabajan en el mercado negro de celulares, desbloqueando, clonando o programando nuevamente los celulares robados.

FTP:

FTP (File Transfer Protocol) es un protocolo de transferencia de archivos entre sistemas conectados a una red TCP basado en la arquitectura cliente-servidor, de manera que desde un equipo cliente nos podemos conectar a un servidor para descargar archivos desde él o para enviarle nuestros propios archivos independientemente del sistema operativo utilizado en cada equipo. El Servicio FTP es ofrecido por la capa de Aplicación del modelo de capas de red TCP/IP al usuario, utilizando normalmente el puerto de red 20 y el 21. Un problema básico de FTP es que está pensado para ofrecer la máxima velocidad en la conexión, pero no la máxima seguridad, ya que todo el intercambio de información, desde el login y password del usuario en el servidor hasta la transferencia de cualquier archivo, se realiza en texto plano sin ningún tipo de cifrado, con lo que un posible atacante lo tiene muy fácil para capturar este tráfico, acceder al servidor, o apropiarse de los archivos transferidos. Para solucionar este problema son de gran

SEGU-INFO.COM.AR

utilidad aplicaciones como scp y sftp, incluidas en el paquete SSH, que permiten transferir archivos pero cifrando todo el tráfico.

GATEWAY:

En telecomunicaciones, el término gateway puede referirse a:

Una puerta de enlace, un nodo en una red informática que sirve de punto de acceso a otra red.

Una pasarela, un dispositivo dedicado a intercomunicar sistemas de protocolos incompatibles.

Puerta de Enlace:

Un puerta de enlace o gateway es normalmente un equipo informático configurado para dotar a las máquinas de una red local (LAN) conectadas a él de un acceso hacia una red exterior, generalmente realizando para ello operaciones de traducción de direcciones IP (NAT: Network Address Translation). Esta capacidad de traducción de direcciones permite aplicar una técnica llamada IP Masquerading (enmascaramiento de IP), usada muy a menudo para dar acceso a Internet a los equipos de una red de área local compartiendo una única conexión a Internet, y por tanto, una única dirección IP externa. Se podría decir que un gateway es un router que conecta dos redes. La dirección IP de un gateway a menudo se parece a 192.168.100.1.

GESTIÓN DE CLAVES:

Controles referidos a la gestión de claves criptográficas.

GESTIÓN DEL RIESGO:

Proceso de identificación, control y mitigación o eliminación, a costo aceptable, de los riesgos que afecten a los sistemas de información de la compañía.

GRE:

Generic Routing Encapsulation (GRE) es un protocolo del nivel de transporte que puede encapsular una amplia variedad de tipos de protocolos diferentes dentro de túneles IP, creando una red punto a punto entre dos máquinas que estén comunicándose por este protocolo. Su uso principal es crear túneles VPN.

GUSANO:

Termino famoso a partir de Robert Morris, Jr. Los Gusanos son programas que se reproducen ellos mismos copiándose una y otra vez de sistema a sistema y que usa recursos de los sistemas atacados.

HARDENING:

Hardening es una acción compuesta por un conjunto de actividades que son llevadas a cabo por el administrador de un sistema operativo para reforzar al máximo posible la seguridad de su equipo. Su propósito, entorpecer la labor del atacante y ganar tiempo para poder minimizar las consecuencias de un inminente incidente de seguridad e incluso, en algunos casos, evitar que éste se concrete en su totalidad. Una de las primeras cosas que hay que dejar en claro del Hardening de sistemas operativos es que no necesariamente logrará forjar equipos invulnerables. Es importante recordar que, según el modelo de defensa en profundidad, el host es sólo una capa de éste. En otras palabras, un factor más a considerar dentro del gran número de puntos a ser tomados en cuenta para defender globalmente un sistema.

SEGU-INFO.COM.AR

Entre las actividades propias de un proceso de hardening se pueden contar las siguientes:

• **Configuraciones necesarias para protegerse de posibles ataques físicos o de hardware de la máquina**. Entre otras actividades, destacan el upgrade de firmware, el establecimiento de contraseñas complejas para el arranque del equipo y la configuración de la BIOS, la deshabilitación de inicio de sistema para cualquier unidad que no sea el disco duro principal, y en casos de servidores, la deshabilitación de dispositivos ópticos, USB o similares, para evitar cualquier entrada de malware desde un medio de almacenamiento externo.

• **Instalación segura del sistema operativo**. Esto implica, entre otras cosas, el considerar al menos dos particiones primarias (una para el sistema operativo en sí y otra para carpetas y archivos de importancia), el uso de un sistema de archivos que tenga prestaciones de seguridad, y el concepto de instalación mínima, es decir, evitando la instalación de cualquier componente de sistema que no sea necesario para el funcionamiento del sistema.

• **Activación y/o configuración adecuada de servicios de actualizaciones automáticas**, para asegurar que el equipo tendrá todos los parches de seguridad que entrega el proveedor al día. En caso de que se encuentre dentro de una corporación, es adecuado instalar un servidor de actualizaciones, que deberá probar en un entorno de laboratorio el impacto de la instalación de actualizaciones antes de instalarlas en producción.

• **Instalación, configuración y mantenimiento de programas de seguridad** tales como antivirus, antispyware, y un filtro antispam según las necesidades del sistema.

• **Configuración de la política local del sistema**, considerando varios puntos relevantes:

  o **Política de contraseñas robusta**, con claves caducables, almacenamiento histórico de contraseñas (para no usar contraseñas cíclicas), bloqueos de cuentas por intentos erróneos y requisitos de complejidad de contraseñas.

  o **Renombramiento y posterior deshabilitación de cuentas estándar del sistema**, como administrador e invitado.

  o **Asignación correcta de derechos de usuario**, para reducir las posibilidades de elevación de privilegios, y tratando siempre de limitar al mínimo los privilegios y/o derechos de los usuarios activos.

  o **Configuración de opciones de seguridad generales**, como aquellas relacionadas con rutas de acceso compartido, apagado de sistema, inicio y cierre de sesión y opciones de seguridad de red.

  o **Restricciones de software**, basado en lo posible en el uso de listas blancas de software permitido más que en listas negras del mismo.

  o **Activación de auditorias de sistema**, claves para tener un registro de algunos intentos de ataque característicos como la adivinación de contraseñas.

• **Configuración de servicios de sistema**. En este punto es necesario tratar siempre de deshabilitar todos aquellos servicios que no vayan a prestar una funcionalidad necesaria para el funcionamiento del sistema. Por ejemplo, si su equipo no posee tarjetas de red inalámbrica, el servicio de redes inalámbricas debería estar deshabilitado.

• **Configuración de los protocolos de Red**. En la medida de lo posible, es recomendable usar sistemas de traducción de direcciones (NAT) para direccionar los equipos internos de una organización. Deshabilitar todos aquellos protocolos de red innecesarios en el sistema y limitar el uso de los mismos al mínimo. TCP/IP es un protocolo que no nació pensando en seguridad, por lo que limitar su uso al estrictamente necesario es imperativo.

SEGU-INFO.COM.AR

• **Configuración adecuada de permisos de seguridad en archivos y carpetas del sistema**. En la medida de lo posible, denegar explícitamente cualquier permiso de archivo a las cuentas de acceso anónimos o que no tengan contraseña. Un correcto set de permisos a nivel de carpetas y archivos es clave para evitar acceso no deseado al contenido de los mismos.

• **Configuración de opciones de seguridad de los distintos programas**, como clientes de correo electrónico, navegadores de Internet y en general de cualquier tipo de programa que tenga interacción con la red.

• **Configuración de acceso remoto**. En caso de no ser estrictamente necesario, es bueno deshabilitar el acceso remoto. Sin embargo, cuando es necesario tener control remoto de la máquina, es preciso configurarlo de manera adecuada, restringiendo el acceso a un número muy limitado de usuario, restringiendo al mínimo las conexiones concurrentes, tomando cuidado en la desconexión y cierre de sesión y estableciendo un canal cifrado de comunicaciones para tales propósitos, como SSH.

• **Configuración adecuada de cuentas de usuario**, tratando de trabajar la mayor parte del tiempo con cuentas de acceso limitado y deshabilitando las cuentas de administrador. Es absolutamente recomendable usar la impersonificación de usuarios para realizar labores administrativas en vez de iniciar sesión como administradores.

• **Cifrado de archivos o unidades según las necesidades del sistema**, considerando un almacenamiento externo para las llaves de descifrado. Considerar además la opción de trabajar con sistemas de cifrado de mensajería instantánea y correo electrónico.

• **Realizar y programar un sistema de respaldos frecuente a los archivos y al estado de sistema**. En la medida de lo posible, administrar los respaldos vía red o llevar los respaldos a unidades físicas que estén alejadas del equipo que las origina.

Como conclusión, el Hardening es una ayuda indispensable para ahorrarse bastantes dolores de cabeza por parte de los administradores de sistemas. Entre sus ventajas, se puede contar la disminución por incidentes de seguridad, mejoras en el rendimiento al disminuir niveles de carga inútil en el sistema, una administración más simple y mayor rapidez en la identificación de problemas, ya que muchas de las posibles causas de ellos quedarán descartadas en virtud de las medidas tomadas, y finalmente la posibilidad –en muchos casos– de poder hacer un seguimiento de los incidentes y en algunos casos identificar el origen de los mismos. Es un trabajo que no es trivial, y que bien vale la pena hacerlo.

HTTP:

El protocolo de transferencia de hipertexto (HTTP, HyperText Transfer Protocol) es el protocolo usado en cada transacción de la Web (WWW). HTTP fue desarrollado por el consorcio W3C y la IETF, colaboración que culminó en 1999 con la publicación de una serie de RFC, siendo el más importante de ellos el RFC 2616, que especifica la versión 1.1.

HTTP define la sintaxis y la semántica que utilizan los elementos software de la arquitectura web (clientes, servidores, proxies) para comunicarse. Es un protocolo orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor. Al cliente que efectúa la petición (un navegador o un spider) se lo conoce como "user agent" (agente del usuario). A la información transmitida se la llama recurso y se la identifica mediante un URL. Los recursos pueden ser archivos, el resultado de la ejecución de un programa, una consulta a una base de datos, la traducción automática de un documento, etc.

HTTP es un protocolo sin estado, es decir, que no guarda ninguna información sobre conexiones anteriores. El desarrollo de aplicaciones web necesita frecuentemente mantener estado. Para esto se usan las cookies, que es información que un servidor puede almacenar en el sistema cliente. Esto le permite a las aplicaciones web instituir la noción de "sesión", y también permite rastrear usuarios ya que las cookies pueden guardarse en el cliente por tiempo indeterminado.

HTTPS:

SEGU-INFO.COM.AR

El protocolo HTTPS es la versión segura del protocolo HTTP. El sistema HTTPS utiliza un cifrado basado en las Secure Socket Layers (SSL) para crear un canal cifrado (cuyo nivel de cifrado depende del servidor remoto y del navegador utilizado por el cliente) más apropiado para el tráfico de información sensible que el protocolo HTTP. Cabe mencionar que el uso del protocolo HTTPS no impide que se pueda utilizar HTTP. Es aquí, cuando nuestro navegador nos advertirá sobre la carga de elementos no seguros (HTTP), estando conectados a un entorno seguro (HTTPS). Es utilizado principalmente por entidades bancarias, tiendas en línea, y cualquier tipo de servicio que requiera el envío de datos personales o contraseñas. El puerto estándar para este protocolo es el 443.

HACKER:

Persona que tiene un conocimiento profundo acerca del funcionamiento de redes, sistemas operativos, comunicaciones, protocolos, tecnologías y que puede advertir los errores y fallas de seguridad de los mismos.

Hacker es el neologismo utilizado para referirse a un experto en varias o alguna rama técnica relacionada con la informática: programación, redes de computadoras, sistemas operativos, hardware de red/voz, etc. Se suele llamar hackeo y hackear a las obras propias de un hacker.

El término "Hacker" trasciende a los expertos relacionados con la informática, para también referirse a cualquier profesional que está en la cúspide de la excelencia en su profesión, ya que en la descripción más pura, un hacker es aquella persona que le apasiona el conocimiento, descubrir o aprender nuevas cosas y entender el funcionamiento de éstas.

HP/UX:
Sistema operativo de HP.

HOAX:

Mensaje de correo electrónico creado para un reenvío masivo que intenta hacer creer al remitente algo que es falso. El Hoax más común es para alertar de virus inexistentes.

HUB:

Un concentrador es un dispositivo que permite centralizar el cableado de una red. También conocido con el nombre de hub.

Un concentrador funciona repitiendo cada paquete de datos en cada uno de los puertos con los que cuenta, excepto en el que ha recibido el paquete, de forma que todos los puntos tienen acceso a los datos. También se encarga de enviar una señal de choque a todos los puertos si detecta una colisión. Son la base para las redes de topología tipo estrella. Como alternativa existen los sistemas en los que los ordenadores están conectados en serie, es decir, a una línea que une varios o todos los ordenadores entre sí, antes de llegar al ordenador central. Llamado también repetidor multipuerto, existen 3 clases:

- Pasivo: No necesita energía eléctrica.
- Activo: Necesita alimentación.
- Inteligente: También llamados smart hubs son hubs activos que incluyen microprocesador.

Dentro del modelo OSI el concentrador opera a nivel 1 de la capa física, al igual que los repetidores, y puede ser implementado utilizando únicamente tecnología analógica. Simplemente une conexiones y no altera las tramas que le llegan.

Visto lo anterior podemos sacar las siguientes conclusiones:

El concentrador envía información a ordenadores que no están interesados. A este nivel sólo hay un destinatario de la información, pero para asegurarse de que la recibe el

SEGU-INFO.COM.AR

concentrador envía la información a todos los ordenadores que están conectados a él, así seguro que acierta.

Este tráfico añadido genera más probabilidades de colisión. Una colisión se produce cuando un ordenador quiere enviar información y emite de forma simultánea con otro ordenador que hace lo mismo. Al chocar los dos mensajes se pierden y es necesario retransmitir. Además, a medida que añadimos ordenadores a la red también aumentan las probabilidades de colisión.

Un concentrador funciona a la velocidad del dispositivo más lento de la red. Si observamos cómo funciona vemos que el concentrador no tiene capacidad de almacenar nada. Por lo tanto si un ordenador que emite a 100 megabit/segundo le trasmitiera a otro de 10 megabit/segundo algo se perdería del mensaje. En el caso del ADSL los routers suelen funcionar a 10 megabit/segundo, si lo conectamos a nuestra red casera, toda la red funcionará a 10 megabit/segundo, aunque nuestras tarjetas sean 10/100 megabit/segundo.

Un concentrador es un dispositivo simple, esto influye en dos características. El precio es barato. Un concentrador casi no añade ningún retardo a los mensajes.

Los concentradores fueron muy populares hasta que se abarataron los switch que tienen una función similar pero proporcionan más seguridad contra programas como los sniffer. La disponibilidad de switches ethernet de bajo precio ha dejado obsoletos, pero aún se pueden encontrar en instalaciones antiguas y en aplicaciones especializadas.

IDS:

Un sistema de detección de intrusos (o IDS de sus siglas en inglés Intrusion Detection System) es un programa usado para detectar accesos desautorizados a un computador o a una red. Estos accesos pueden ser ataques de habilidosos hackers, o de Script Kiddies que usan herramientas automáticas.

El IDS suele tener sensores virtuales (por ejemplo, un sniffer de red) con los que el núcleo del IDS puede obtener datos externos (generalmente sobre el tráfico de red). El IDS detecta, gracias a dichos sensores, anomalías que pueden ser indicio de la presencia de ataques o falsas alarmas.

ICMP:

El Protocolo de Control de Mensajes de Internet (ICMP por sus siglas en inglés) es uno de los protocolos centrales de la suite de protocolos de Internet. Es usado principalmente por los Sistemas operativos de las computadoras en una red para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado.

ICMP difiere del propósito de TCP y UDP ya que generalmente no se utiliza directamente por las aplicaciones de usuario en la red. La única excepción es la herramienta ping, que envía mensajes de petición Echo ICMP (y recibe mensajes de respuesta Echo) para determinar si un host está disponible y el tiempo que le toma a los paquetes en ir y regresar a ese host.

Aspectos Técnicos:

El Protocolo de Control de Mensajes de Internet (Internet Control Message Protocol-ICMP por sus siglas en inglés) es parte de la Suite IP tal cual y se definió en la RFC 792. Los mensajes ICMP son comúnmente generados en respuesta a errores en los datagramas de IP (según la especificación RFC 1122) ó para diagnostico y ruteo.

La versión de ICMP para IPv4 también es conocida como ICMPv4. IPv6 tiene su protocolo equivalente.

SEGU-INFO.COM.AR

Los mensajes ICMP son construidos al nivel de capa de red. IP encapsula el mensaje ICMP apropiado con una nueva cabecera IP (para obtener los mensajes de respuesta desde el host original que envía), y transmite el datagrama resultante de manera habitual.

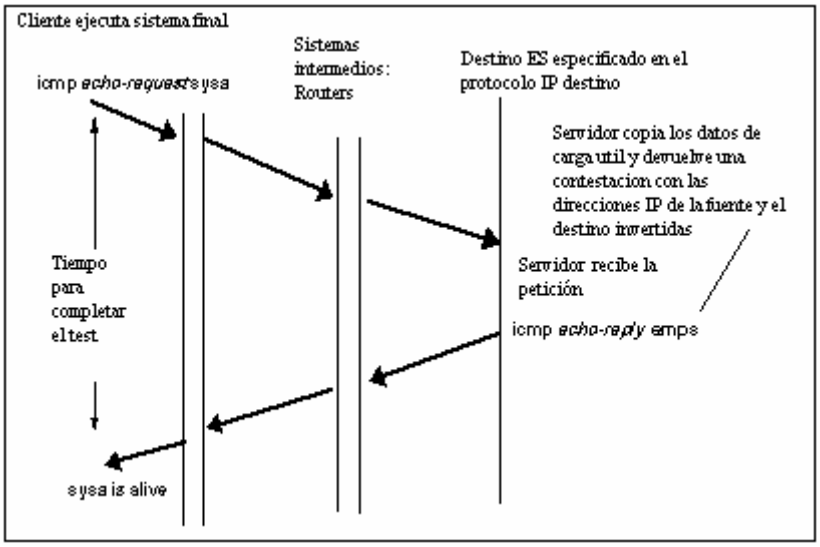
Por ejemplo, cada router que reenvía un datagrama IP tienen que disminuir el campo de tiempo de vida (TTL) de la cabecera IP en uno; si el TTL llega a 0, un mensaje ICMP "Tiempo de Vida se ha excedido en transmitirse" es enviado a la fuente del datagrama.

Cada mensaje ICMP es enscapsulado directamente en un solo datagrama IP, y por tanto no garantiza la entrega del ICMP.

Aunque los mensajes ICMP son contenidos dentro de datagramas estándar IP, los mensajes ICMP se procesan como un caso especial del procesamiento normal de IP, algo así como el procesamiento de un sub-protocolo de IP. En muchos de los casos, es necesario inspeccionar el contenido del mensaje ICMP, y entregar el mensaje apropiado de error a la aplicación que generó el paquete IP original, aquel que incitó al envío del mensaje ICMP.

La utilidad del protocolo ICMP es controlar si un paquete no puede alcanzar su destino, si su vida ha expirado etc. Es decir, se usa para manejar mensajes de error y de control necesarios para los sistemas de la red, informando con ellos a la fuente original para que evite o corrija el problema detectado.

Muchas de las utilidades de red comunes están basadas en los mensajes ICMP. El comando traceroute está implementado transmitiendo datagramas UDP con campos especiales TTL IP en la cabecera, y buscando los mensajes de "Tiempo de Vida en tránsito" y "Destino inalcanzable" generados como respuesta. La herramienta ping está implementada utilizando los mensajes "Echo request" y "Echo reply" de ICMP.



Ejemplo de envío y recepción de un ping. Lista de mensajes de control permitidos (incompleta):

SEGU-INFO.COM.AR

0 - Echo Reply
1 - Reservado
2 - Reservado
3 - Destination Unreachable
4 - Source Quench
5 - Redirect Message
6 - Dirección Alterna de Host
7 - Reservado
8 - Echo Request
9 - Anuncio de Router
10 - Solicitud de Router
11 - Tiempo Excedido
12 - Problema de Parámetro
13 - Marca de tiempo
14 - Respuesta de Marca de tiempo
15 - Petición de Información
16 - Respuesta de Información
17 - Petición de Máscara de Dirección
18 - Respuesta de Máscara de Dirección
19 - Reservado para seguridad
20-29 - Reservado para experimentos de robustez
30 - Traceroute
31 - Error de Conversión de Datagrama
32 - Redirección de Host Móvil
33 - ¿IPv6 Donde estas?
34 - ¿IPv6 Donde estoy?
35 - Petición de Registro de Móvil
36 - Respuesta de registro de Móvil
37 - Petición de Nombre de Dominio
38 - Respuesta de Nombre de Dominio
39 - SKIP Protocolo de Algoritmo de Descubrimiento
40 - Photuris, Fallas de Seguridad
41 - 255 - Reservado

IMAP:

IMAP (acrónimo inglés de Internet Message Access Protocol) es un protocolo de red de

SEGU-INFO.COM.AR

acceso a mensajes electrónicos almacenados en un servidor. Mediante IMAP se puede tener acceso al correo electrónico desde cualquier equipo que tenga una conexión a Internet. Una vez configurada la cuenta IMAP es posible especificar las carpetas que se desea mostrar y las que desea ocultar, característica que lo hace diferente del protocolo POP.

IMAP y POP3 (Post Office Protocol versión 3) son los dos protocolos más prevalecientes para la obtención de correo electrónico. Todos los servidores y clientes de email están virtualmente soportados por ambos, aunque en algunos casos hay algunas interfaces específicas del fabricante típicamente propietarias. Por ejemplo, mientras que los protocolos propietarios utilizados entre el cliente Microsoft Outlook y su servidor Microsoft Exchange Server o el cliente Lotus Notes de IBM y el servidor Domino, estos productos también soportan interoperabilidad con IMAP y POP3 con otros clientes y servidores. La versión actual de IMAP, IMAP versión 4 revisión 1 (IMAP4ver1), está definida por el RFC 3501.

INVENTARIO DE ACTIVOS:

Detalle de los recursos físicos, información, software, documentos, servicios, personas, etc. Que tienen valor para la compañía y necesitan ser protegidos de riesgos potenciales.

INTEGRIDAD:

Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

IMPACTO:

El costo para la empresa de un incidente que puede o no ser medido en términos estrictamente financieros. Por ejemplo: perdida de reputación, implicaciones legales.

IP:

El Protocolo de Internet (IP, de sus siglas en inglés Internet Protocol) es un protocolo no orientado a conexión usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados.

Los datos en una red basada en IP son enviados en bloques conocidos como paquetes o datagramas (en el protocolo IP estos términos se suelen usar indistintamente). En particular, en IP no se necesita ninguna configuración antes de que un equipo intente enviar paquetes a otro con el que no se había comunicado antes.

El Protocolo de Internet provee un servicio de datagramas no fiable (también llamado del mejor esfuerzo (best effort), lo hará lo mejor posible pero garantizando poco). IP no provee ningún mecanismo para determinar si un paquete alcanza o no su destino y únicamente proporciona seguridad (mediante checksums o sumas de comprobación) de sus cabeceras y no de los datos transmitidos. Por ejemplo, al no garantizar nada sobre la recepción del paquete, éste podría llegar dañado, en otro orden con respecto a otros paquetes, duplicado o simplemente no llegar. Si se necesita fiabilidad, esta es proporcionada por los protocolos de la capa de transporte, como TCP.

Si la información a transmitir ("datagramas") supera el tamaño máximo "negociado" (MTU) en el tramo de red por el que va a circular podrá ser dividida en paquetes más pequeños, y reensamblada luego cuando sea necesario. Estos fragmentos podrán ir cada uno por un camino diferente dependiendo de como estén de congestionadas las rutas en cada momento.

Las cabeceras IP contienen las direcciones de las máquinas de origen y destino (direcciones IP), direcciones que serán usadas por los conmutadores de paquetes (switches) y los enrutadores (routers) para decidir el tramo de red por el que reenviarán los paquetes.

El IP es el elemento común en la Internet de hoy. El actual y más popular protocolo de red es IPv4. IPv6 es el sucesor propuesto de IPv4; poco a poco Internet está agotando las direcciones disponibles por lo que IPv6 utiliza direcciones de fuente y destino de 128 bits (lo cuál asigna a cada milímetro cuadrado de la superficie de la Tierra la colosal cifra de 670 mil billones

SEGU-INFO.COM.AR

de direcciones IP's), muchas mas direcciones que las que provee IPv4 con 32 bits. Las versiones de la 0 a la 3 están reservadas o no fueron usadas. La versión 5 fue usada para un protocolo experimental. Otros números han sido asignados, usualmente para protocolos experimentales, pero no han sido muy extendidos.

IPS:

Un Sistema de Prevención de Intrusos (IPS) es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos. La tecnología de Prevención de Intrusos es considerada por algunos como una extensión de los Sistemas de Detección de Intrusos (IDS), pero en realidad es otro tipo de control de acceso, más cercano a las tecnologías cortafuegos. Los IPS fueron inventados de forma independiente por Jed Haile y Vern Paxon para resolver ambigüedades en el monitoreo pasivo de redes de computadoras, al situar sistemas de detecciones en la vía del tráfico. Los IPS presentan una mejora importante sobre las tecnologías de cortafuegos tradicionales, al tomar decisiones de control de acceso basados en los contenidos del tráfico, en lugar de direcciones IP o puertos. Tiempo después, algunos IPS fueron comercializados por la empresa One Secure, la cual fue finalmente adquirida por NetScreen Technologies, que a su vez fue adquirida por Juniper Networks en 2004. Dado que los IPS fueron extensiones literales de los sistemas IDS, continúan en relación. También es importante destacar que los IPS pueden actuar al nivel de equipo, para combatir actividades potencialmente maliciosas.

IRIX:
Sistema operativo.

ISP (Internet Services Provider):

Proveedor de servicios Internet.

JAMMING o FLOODING:

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

Muchos ISPs (proveedores de Internet) han sufrido bajas temporales del servicio por ataques que explotan el protocolo TCP. Aquí el atacante satura el sistema con mensajes que requieren establecer conexión. Sin embargo, en vez de proveer la dirección IP del emisor, el mensaje contiene falsas direcciones IP (o sea que este ataque involucra también spoofing). El sistema responde al mensaje, pero como no recibe respuesta, acumula buffers con información de las conexiones abiertas, no dejando lugar a las conexiones legítimas.

Muchos host de Internet han sido dados de baja por el "ping de la muerte", una versión-trampa del comando ping. Mientras que el ping normal simplemente verifica si un sistema esta enlazado a la red, el ping de la muerte causa el reboot o el apagado instantáneo del equipo.

Otra acción común es la de enviar millares de e-mails sin sentido a todos los usuarios posibles en forma continua, saturando los distintos servers destino.

JOKE:

Aplicaciones inofensivas que simulan ser virus informáticos. Su fin primordial es gastar una broma a quien las recibe y las ejecuta.

KEY o Llave:

Se puede traducir por clave de acceso a un software o sistema.

KEYLOGGER:

SEGU-INFO.COM.AR

Programa que intercepta todas las pulsaciones realizadas en el teclado para obtener datos sensibles como contraseñas, etc. Posteriormente puede ser enviado a un tercero sin conocimiento ni consentimiento del usuario.

KERBEROS:
Sistema de seguridad (autenticación) en el que los login y los passwords van encriptados.

LAMMER o SCRIPT KIDDIES:

Es un término coloquial inglés aplicado a una persona falta de madurez, sociabilidad y habilidades técnicas o inteligencia, un incompetente, por lo general pretenden hacer hacking sin tener conocimientos de informática. Solo se dedican a buscar y descargar programas de hacking para luego ejecutarlos, como resultado de la ejecución de los programas descargados estos pueden terminar colapsando sus sistemas por lo general destrozando su plataforma en la que trabajan.

Son aprendices que presumen de lo que no son, aprovechando los conocimientos del hacker y lo ponen en práctica sin saber, en palabras no saben nada de hacker.

LEY:

Regla, norma. Disposición emanada por el poder legislativo.

LINUX:
Sistema operativo de la familia UNIX

LOGIN:
Para entrar en un sistema por telnet se necesita siempre un login (nombre) y un password (clave).

LUSER (looser + user):

Es un término utilizado por hackers para referirse a los usuarios comunes, de manera despectiva y como burla. "Luser", que generalmente se encuentra en desventaja frente a os usuarios expertos (hackers), quienes pueden controlar todos los aspectos de un sistema.

MAIL BOMBER:

Consiste en el envío masivo de mails a una dirección (para lo que hay programas destinados al efecto) con la consiguiente problemática asociada para la víctima.

MD5:

Operación unidireccional que transforma una cadena de datos de cualquier longitud en otra cadena mas corta de longitud fija, la suma de comprobación de la función MD5 verifica la integridad de los datos.

MIME:

MIME (Multipurpose Internet Mail Extensions, Extensiones de Correo Internet Multipropósito), son una serie de convenciones o especificaciones dirigidas a que se puedan intercambiar a través de Internet todo tipo de archivos (texto, audio, vídeo, etc.) de forma transparente para el usuario. Una parte importante del MIME está dedicada a mejorar las posibilidades de transferencia de texto en distintos idiomas y alfabetos. En 1991 la IETF (Internet Engineering Task Force) comenzó a desarrollar esta norma y desde 1994 todas las extensiones MIME están especificadas de forma detallada en diversos documentos oficiales disponibles en Internet (RFC 2045-2049). En la actualidad ningún programa de correo electrónico o navegador

SEGU-INFO.COM.AR

de Internet puede considerarse completo si no acepta MIME en sus diferentes facetas (texto y formatos de archivo).

NAT:

NAT (Network Address Translation - Traducción de Dirección de Red) es un estándar creado por la Internet Engineering Task Force (IETF) el cual utiliza una o más direcciones IP para conectar varios computadores a otra red (normalmente a Internet), los cuales tiene una dirección IP completamente distinta (normalmente una IP no válida de Internet definida por el RFC 1918). Por lo tanto, se puede utilizar para dar salida a redes públicas a computadores que se encuentran con direccionamiento privado o para proteger máquinas públicas.

Funcionamiento:

El protocolo TCP/IP tiene la capacidad de generar varias conexiones simultáneas con un dispositivo remoto. Para realizar esto, dentro de la cabecera de un paquete IP, existen campos en los que se indica la dirección origen y destino con sus respectivos puertos. Esta combinación de números define una única conexión.

Una pasarela NAT cambia la dirección origen en cada paquete de salida y, dependiendo del método, también el puerto origen para que sea único. Estas traducciones de dirección se almacenan en una tabla, para recordar que dirección y puerto le corresponde a cada dispositivo cliente y así saber donde deben regresar los paquetes de respuesta. Si un paquete que intenta ingresar a la red interna no existe en la tabla de traducciones, entonces es descartado. Debido a este comportamiento, se puede definir en la tabla que en un determinado puerto y dirección, se pueda acceder a un determinado dispositivo, como por ejemplo un servidor web, lo que se denomina NAT inverso o DNAT (Destination NAT).

NAT tiene muchas formas de funcionamiento, entre las que destaca:

NAT estático

Realiza un mapeo en la que una dirección IP privada se traduce a una correspondiente dirección IP pública de forma unívoca. Normalmente se utiliza cuando un dispositivo necesita ser accesible desde fuera de la red privada.

NAT dinámico

Una dirección IP privada se traduce a un grupo de direcciones públicas. Por ejemplo, si un dispositivo posee la IP 192.168.10.10 puede tomar direcciones de un rango entre la IP 200.85.67.44 y 200.85.67.99. Implementando esta forma de NAT se genera automáticamente un firewall entre la red pública y la privada, ya que sólo se permite la conexión que se origina desde ésta última.

Sobrecarga

La forma más utilizada de NAT, proviene del NAT dinámico ya que toma múltiples direcciones IP privadas (normalmente entregadas mediante DHCP) y las traduce a una única dirección IP pública utilizando diferentes puertos. Esto se conoce también como PAT (Port Address Translation - Traducción de Direcciones por Puerto), NAT de única dirección o NAT multiplexado a nivel de puerto.

Traslape

Cuando las direcciones IP utilizadas en la red privada son direcciones IP públicas en uso en otra red. El ruteador posee una tabla de traducciones en donde se especifica el reemplazo de éstas con una única dirección IP pública. Así se evita los conflictos de

SEGU-INFO.COM.AR

direcciones entre las distintas redes.

Razones de la creación y utilización de NAT

Con el crecimiento exponencial de Internet, y debido a que se utiliza direccionamiento IPv4, el cual ocupa 32 bits para la asignación de direcciones, dando un máximo de 4.294.967.296 direcciones únicas (2 elevado a 32), llegó el momento en que el número de direcciones no daba abasto para la cantidad de dispositivos conectados. Incluso, el número de direcciones es menor al teórico, por la forma en que se distribuyen las direcciones en clases, otras son reservadas para multicasting, y para usos especiales. Para solucionar esto se diseño un protocolo que es capaz de asignar un número mayor de direcciones, llamado IPv6, pero tomará muchos años su implantación, por que hay que modificar completamente la infraestructura de Internet.

Finalmente se diseñó NAT, el cual permite a cualquier dispositivo, como un router, actuar como traductor de direcciones.

NAT es muy utilizado en empresas y redes caseras, ya que basta tener una sola dirección IP pública para poder conectar una multitud de dispositivos.

NDA:

NDA son las siglas en inglés de "Non-Disclosure Agreement", es un contrato legal entre al menos dos entidades para compartir material confidencial o conocimiento para ciertos propósitos, pero restringiendo su uso público. Un NDA crea una relación confidencial entre los participantes para proteger cualquier secreto comercial. Por tanto, un NDA puede proteger información de una empresa privada.

NDAs se firman habitualmente cuando dos empresas o individuos acuerdan alguna relación comercial y necesitan entender los procesos usadas en la otra compañía con el propósito de evaluar el interés de dicha relación. Los NDAs puedes ser mutuos, de modo que las dos partes tienen restricciones de uso de la información proporcionada, o pueden afectar sólo a una de las partes.

También es común que un empleado firme un NDA o acuerdo similar en el momento de su contratación. Son muy comunes en el campo de las IT.

NETBEUI:

NetBEUI (NetBIOS Extended User Interface, en español Interfaz extendida de usuario de NetBIOS), es un protocolo de nivel de red sencillo utilizado en las primeras redes de Microsoft como Lan Manager o en Windows 95. La comunicación entre equipos se consigue gracias al intercambio de sus nombres en una red de área local, pero no dispone de mecanismos para conectar equipos que estén en redes separadas: es un protocolo sin encaminamiento.

NetBEUI, al igual que NetBIOS, corre sobre el protocolo LLC2.

NetBEUI proporciona los servicios de red para NetBIOS; en los sistemas actuales NetBIOS puede funcionar sobre protocolos más completos y extendidos como IPX o el propio IP empleado en la arquitectura TCP/IP de Internet e intranets.

NEWBIE:

La palabra es una probable corrupción de new boy, arquetipo del "niño nuevo", que debido a la falta de interacciones socioculturales, queda vulnerable a varios tipos de abusos por parte de los otros. Son los hacker novatos, se introducen en sistemas de fácil acceso y fracasan en muchos intentos, sólo con el objetivo de aprender las técnicas que puedan hacer de él, un hacker reconocido, se dedica a leer, escuchar, ver y probar las distintas técnicas que va aprendiendo. Sólo pregunta a otros hackers, después de dí-as de pruebas sin resultado, de manera que más que preguntar, expone su experiencia y pide opiniones o deja en el aire preguntas muy concretas. Son más precavidos y cautelosos que los lamers, aprenden de los métodos de hacking, no se mofan con lo que hacen sino sacan provecho en todo lo que aprender, por lo general llegan tanto a apasionarse por la informática, la electrónica y las

SEGU-INFO.COM.AR

telecomunicaciones que aspiran a llegar a ser hacker.

NO CONFORMIDAD:

Situación que evidencia el no cumplimiento de algún control, pudiendo atentar la confidencialidad, integridad o disponibilidad de información sensible o bien representar un riesgo menor.

NO REPUDIO:

Servicio de seguridad que previene que un emisor niegue haber emitido un mensaje, cuando realmente lo ha emitido, y que un receptor niegue su recepción, cuando realmente lo ha recibido.

NUKEAR:
Consiste en hacer caer o desconectar a alguien de un programa en ejecución, como por ejemplo un programa de chat.

NNTP:

Network News Transport Protocol (NNTP), o protocolo de transferencia de noticias. Es el Protocolo de red utilizado por el Usenet internet service. Es un Protocolo de red basado en tiras de textos enviados sobre canales TCP de 7 bit ASCII. Es usado para subir y bajar así como para transferir artículos entre servidores. Hoy en día también algunos BBS usan este protocolo para dejar disponibles sus foros o áreas de correo de la red FidoNet u o tras redes.

OSI:

El modelo de referencia de Interconexión de Sistemas Abiertos (OSI, Open System Interconnection) lanzado en 1984 fue el modelo de red descriptivo creado por ISO; esto es, un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones. Siguiendo el esquema de este modelo se crearon numerosos protocolos, por ejemplo X.25, que durante muchos años ocuparon el centro de la escena de las comunicaciones informáticas. El advenimiento de protocolos más flexibles donde las capas no están tan demarcadas y la correspondencia con los niveles no era tan clara puso a este esquema en un segundo plano. Sin embargo sigue siendo muy usado en la enseñanza como una manera de mostrar como puede estructurarse una "pila" de protocolos de comunicaciones (sin importar su poca correspondencia con la realidad).

El modelo en sí mismo no puede ser considerado una arquitectura, ya que no especifica el protocolo que debe ser usado en cada capa, sino que suele hablarse de modelo de referencia. Este modelo está dividido en siete capas:

1. Capa Física (Capa 1)
    b. Codificación de la señal
    c. Topología y medios compartidos
    d. Equipos adicionales
2. Capa de enlace de datos (Capa 2)
3. Capa de red (Capa 3)
4. Capa de transporte (Capa 4)
5. Capa de sesión (Capa 5)
6. Capa de presentación (Capa 6)
7. Capa de aplicación (Capa 7)

SEGU-INFO.COM.AR

PERITO:

Persona, que poseyendo la facultad y los conocimientos científicos, artísticos, técnicos, informa bajo juramento sobre puntos litigiosos la relación de su experiencia.

PHREAKING:
Consiste en evitar total o parcialmente el pago a las grandes multinacionales El término "Phreak" es una conjunción de las palabras “phone” (teléfono en inglés) y “freak” (monstruo en inglés). También se refiere al uso de varias frecuencias de audio para manipular un sistema telefónico, ya que la palabra phreak se pronuncia de forma similar a “frequency” (frecuencia).

PIRATA:
Persona dedicada a la copia y distribución de software ilegal, tanto software comercial crackeado, como shareware registrado, etc...

PGP:
Pretty Good Privacy. Es un programa desarrollado por Phil Zimmermann y cuya finalidad es proteger la información distribuida a través de Internet mediante el uso de criptografía de clave pública, así como facilitar la autenticación de documentos gracias a firmas digitales.

POLÍTICA DE SEGURIDAD:

Documento que establece el compromiso de la Dirección y el enfoque de la Compañía en la gestión de la seguridad de la información.

POP:

El significado de las siglas POP es Post Office Protocol (Protocolo de Oficina de Correos). El sinonimo de otros protocolos creados con anterioridad como el SMTP el POP no necesita una conexión permanente a internet, puesto que es en el momento de la conexión cuando solicita al servidor el envío de la correspondencia almacenada en el servidor para dicho usuario. Si se está permanentemente conectado a internet pueden configurarse los programas cliente de correo de tal forma que la petición al servidor de correo se efectúe automáticamente cada cierto tiempo y de esta forma avise al usuario de que tiene correo pendiente de recibir. La situación actual es que se utiliza el protocolo SMTP para el envío de correo y para la recepción de correo se utiliza el protocolo POP, pero ya en su tercera versión desde su aparición, el POP3.

PORT SCANNER:

Programa que te indica que puertos de una maquina están abiertos.

PROXY:

En el contexto de las ciencias de la computación, el término proxy hace referencia a un programa o dispositivo que realiza una acción en representación de otro. La finalidad más habitual es la del servidor proxy, que sirve para permitir el acceso a Internet a todos los equipos de una organización cuando sólo se puede disponer de un único equipo conectado, esto es, una única dirección IP.

En general

La palabra proxy se usa en muchas situaciones en donde tiene sentido un intermediario:

El uso más común es el de servidor proxy, que es un ordenador que intercepta las conexiones de red que un cliente hace a un servidor de destino.

De ellos, el más famoso es el servidor proxy de web (comúnmente conocido como sólo "proxy"). Intercepta la navegación de los clientes por páginas web, por varios motivos

SEGU-INFO.COM.AR

posibles: seguridad, rendimiento, anonimato...

También existen proxys para otros protocolos, como el proxy de FTP

El proxy ARP puede hacer de enrutador en una red, ya que hace de intermediario entre ordenadores.

Proxy (patrón de diseño) también es un patrón de diseño (programación) con el mismo esquema que el proxy de red.

Un componente hardware también puede actuar como intermediario para otros (por ejemplo, un teclado USB al que se le pueden conectar más dispositivos USB).

Fuera de la informática, un proxy puede ser una persona autorizada para actuar en representación de otra persona; por ejemplo, alguien a quien le han delegado el derecho a voto.

Una guerra proxy es una en la que las dos potencias usan a terceros para el enfrentamiento directo.

Como se ve, proxy tiene un significado muy general, aunque siempre es sinónimo de intermediario. También se puede traducir por delegado o apoderado (el que tiene el poder).

Ventajas

En general (no sólo en informática), los proxys hacen posibles varias cosas nuevas:

- Control. Sólo el intermediario hace el trabajo real, por tanto se pueden limitar y restringir los derechos de los usuarios, y dar permisos sólo al proxy.
- Ahorro. Por tanto, sólo uno de los usuarios (el proxy) ha de estar equipado para hacer el trabajo real.
- Velocidad. Si varios clientes van a pedir el mismo recurso, el proxy puede hacer caché: guardar la respuesta de una petición para darla directamente cuando otro usuario la pida. Así no tiene que volver a contactar con el destino, y acaba más rápido.
- Filtrado. El proxy puede negarse a responder algunas peticiones si detecta que están prohibidas.
- Modificación. Como intermediario que es, un proxy puede falsificar información, o modificarla siguiendo un algoritmo.
- Anonimato. Si todos los usuarios se identifican como uno sólo, es difícil que el recurso accedido pueda diferenciarlos. Pero esto puede ser malo, por ejemplo cuando hay que hacer necesariamente la identificación.

Desventajas

En general (no sólo en informática), el uso de un intermediario puede provocar:

- Abuso. Al estar dispuesto a recibir peticiones de muchos usuarios y responderlas, es posible que haga algún trabajo que no toque. Por tanto, ha de controlar quién tiene acceso y quién no a sus servicios, cosa que normalmente es muy difícil.
- Carga. Un proxy ha de hacer el trabajo de muchos usuarios.
- Intromisión. Es un paso más entre origen y destino, y algunos usuarios pueden no querer pasar por el proxy. Y menos si hace de caché y guarda copias de los datos.
- Incoherencia. Si hace de caché, es posible que se equivoque y dé una respuesta antigua cuando hay una más reciente en el recurso de destino.
- Irregularidad. El hecho de que el proxy represente a más de un usuario da problemas en muchos escenarios, en concreto los que presuponen una comunicación directa entre 1 emisor y 1 receptor (como TCP/IP).

SEGU-INFO.COM.AR

Funcionamiento

A continuación se hablará del servidor proxy de web, el más común.

Un proxy permite a otros equipos conectarse a una red de forma indirecta a través de él. Cuando un equipo de la red desea acceder a una información o recurso, es realmente el proxy quien realiza la comunicación y a continuación traslada el resultado al equipo inicial. En unos casos esto se hace así porque no es posible la comunicación directa y en otros casos porque el proxy añade una funcionalidad adicional, como puede ser la de mantener los resultados obtenidos (por ej.: una página web) en una cache que permita acelerar sucesivas consultas coincidentes. Con esta denominación general de proxy se agrupan diversas técnicas.

Proxy de web / Proxy cache de web

Se trata de un proxy para una aplicación específica: el acceso a la web. Aparte de la utilidad general de un proxy, proporciona una cache para las páginas web y los contenidos descargados, que es compartida por todos los equipos de la red, con la consiguiente mejora en los tiempos de acceso para consultas coincidentes. Al mismo tiempo libera la carga de los enlaces hacia Internet.

Funcionamiento

El cliente realiza una petición (por ej.: mediante un navegador web) de un recurso de Internet (una página web o cualquier otro archivo) especificado por una URL.

Cuando el proxy caché recibe la petición, busca la URL resultante en su caché local. Si la encuentra, devuelve el documento inmediatamente, si no es así, lo captura del servidor remoto, lo devuelve al que lo pidió y guarda una copia en su caché para futuras peticiones.

El caché utiliza normalmente un algoritmo para determinar cuándo un documento está obsoleto y debe ser eliminado de la caché, dependiendo de su antigüedad, tamaño e histórico de acceso. Dos de esos algoritmos básicos son el LRU (el usado menos recientemente, en inglés "Least Recently Used") y el LFU (el usado menos frecuentemente, "Least Frequently Used").

Los proxies web también pueden filtrar el contenido de las páginas Web servidas. Algunas aplicaciones que intentan bloquear contenido Web ofensivo están implementadas como proxies Web. Otros tipos de proxy cambian el formato de las páginas web para un propósito o una audiencia específicos, para, por ejemplo, mostrar una página en un teléfono móvil o una PDA. Algunos operadores de red también tienen proxies para interceptar virus y otros contenidos hostiles servidos por páginas Web remotas.

Ejemplo

Un cliente de un ISP manda una petición a Google la petición llega en un inicio al servidor Proxy que tiene este ISP, no va directamente a la dirección IP del dominio de Google. Esta página concreta suele ser muy solicitada por un alto porcentaje de usuarios, por lo tanto el ISP la retiene en su Proxy por un cierto tiempo y crea una respuesta mucho menor en tiempo. Cuando el usuario crea una búsqueda el servidor Proxy ya no es utilizado y megared envía su petición y el cliente recibe su respuesta ahora sí desde Google.

Otros usos

Como método extra y de ayuda en las descargas mediante aplicaciones P2P; el cual es usado en Lphant y algunos Mods del Emule.

SEGU-INFO.COM.AR

Ventajas

- Ahorro de Tráfico: Las peticiones de páginas Web se hacen al servidor Proxy y no a Internet directamente. Por lo tanto, aligera el tráfico en la red y descarga los servidores destino, a los que llegan menos peticiones.
- Velocidad en Tiempo de respuesta: El servidor Proxy crea un caché que evita transferencias idénticas de la información entre servidores durante un tiempo (configurado por el administrador) así que el usuario recibe una respuesta más rápida.
- Demanda a Usuarios: Puede cubrir a un gran número de usuarios, para solicitar, a través de él, los contenidos Web.
- Filtrado de contenidos: El servidor proxy puede hacer un filtrado de páginas o contenidos en base a criterios de restricción establecidos por el administrador dependiendo valores y características de lo que no se permite, creando una restricción cuando sea necesario.
- Modificación de contenidos: En base a la misma función del filtrado, y llamado Privoxy, tiene el objetivo de proteger la privacidad en Internet, puede ser configurado para bloquear direcciones y Cookies por expresiones regulares y modifica en la petición el contenido.

Desventajas

Las páginas mostradas pueden no estar actualizadas si éstas han sido modificadas desde la última carga que realizó el proxy caché.

Un diseñador de páginas web puede indicar en el contenido de su web que los navegadores no hagan una caché de sus páginas, pero este método no funciona habitualmente para un proxy.

El hecho de acceder a Internet a través de un Proxy, en vez de mediante conexión directa, impide realizar operaciones avanzadas a través de algunos puertos o protocolos.

Almacenar las páginas y objetos que los usuarios solicitan puede suponer una violación de la intimidad para algunas personas.

Proxies transparentes

Muchas organizaciones (incluyendo empresas, colegios y familias) usan los proxies para reforzar las políticas de uso de la red o para proporcionar seguridad y servicios de caché. Normalmente, un proxy Web o NAT no es transparente a la aplicación cliente: debe ser configurada para usar el proxy, manualmente. Por lo tanto, el usuario puede evadir el proxy cambiando simplemente la configuración.

Un proxy transparente combina un servidor proxy con NAT de manera que las conexiones son enrutadas dentro del proxy sin configuración por parte del cliente, y habitualmente sin que el propio cliente conozca de su existencia. Este es el tipo de proxy que utilizan los proveedores de servicios de internet (ISP). En España, la compañía más expandida en cuanto a ADSL se refiere, ISP Telefónica, dejó de utilizar proxy transparente con sus clientes a partir de Febrero de 2006.

Reverse Proxy

Un reverse proxy es un servidor proxy instalado en el domicilio de uno o más servidores web. Todo el tráfico entrante de Internet y con el destino de uno de esos servidores web pasa a través del servidor proxy. Hay varias razones para instalar un "reverse proxy":

SEGU-INFO.COM.AR

Seguridad: el servidor proxy es una capa adicional de defensa y por lo tanto protege los servidores web.

Encriptación / Aceleración SSL: cuando se crea un sitio web seguro, habitualmente la encriptación SSL no la hace el mismo servidor web, sino que es realizada por el "reverse proxy", el cual está equipado con un hardware de aceleración SSL (Security Sockets Layer).

Distribución de Carga: el "reverse proxy" puede distribuir la carga entre varios servidores web. En ese caso, el "reverse proxy" puede necesitar reescribir las URL de cada página web (traducción de la URL externa a la URL interna correspondiente, según en qué servidor se encuentre la información solicitada)

Caché de contenido estático: Un "reverse proxy" puede descargar los servidores web almacenando contenido estático como imágenes y otro contenido gráfico.

Proxy NAT (Network Address Translation) / Enmascaramiento

Otro mecanismo para hacer de intermediario en una red es el NAT.

La traducción de direcciones de red (NAT, Network Address Translation) también es conocida como enmascaramiento de IPs. Es una técnica mediante la cual las direcciones fuente o destino de los paquetes IP son reescritas, sustituidas por otras (de ahí el "enmascaramiento").

Esto es lo que ocurre cuando varios usuarios comparten una única conexión a Internet. Se dispone de una única dirección IP pública, que tiene que ser compartida. Dentro de la red de área local (LAN) los equipos emplean direcciones IP reservadas para uso privado y será el proxy el encargado de traducir las direcciones privadas a esa única dirección pública para realizar las peticiones, así como de distribuir las páginas recibidas a aquel usuario interno que la solicitó.

Esta situación es muy común en empresas y domicilios con varios ordenadores en red y un acceso externo a Internet. El acceso a Internet mediante NAT proporciona una cierta seguridad, puesto que en realidad no hay conexión directa entre el exterior y la red privada, y así nuestros equipos no están expuestos a ataques directos desde el exterior.

Mediante NAT también se puede permitir un acceso limitado desde el exterior, y hacer que las peticiones que llegan al proxy sean dirigidas a una máquina concreta que haya sido determinada para tal fin en el propio proxy.

La función de NAT reside en los Cortafuegos (informática), y resulta muy cómoda porque no necesita de ninguna configuración especial en los equipos de la red privada que pueden acceder a través de él como si fuera un mero encaminador.

RARP:

RARP son las siglas en inglés de Reverse Address Resolution Protocol (Protocolo de resolución de direcciones inverso). Es un protocolo utilizado para resolver la dirección IP de una dirección hardware dada (como una dirección Ethernet). La principal limitación era que cada MAC tenía que ser configurada manualmente en un servidor central, y se limitaba solo a la dirección IP, dejando otros datos como la máscara de subred, puerta de enlace y demás información que tenían que ser configurados a mano. Otra desventaja de este protocolo es que utiliza como dirección destino, evidentemente, una dirección MAC de difusión para llegar al servidor RARP. Sin embargo, una petición de ese tipo no es reenviada por el router del segmento de subred local fuera de la misma, por lo que este protocolo, para su correcto funcionamiento, requiere de un servidor RARP en cada subred.

Posteriormente el uso de BOOTP lo dejó obsoleto, ya que éste ya funciona con paquetes UDP, los cuales se reenvían a través de los routers (eliminando la necesidad de disponer de un servidor BOOTP en cada subred) y, además, BOOTP ya tiene un conjunto de funciones mayor que permite obtener más información y no sólo la dirección IP.

SEGU-INFO.COM.AR

RED PRIVADA VIRTUAL:

Red de información privada que hace uso de una red pública, como internet, al encriptar información en un nodo y utilizar procedimientos de seguridad que proporcionan un túnel a través del cual la información puede pasar a otro nodo.

RIESGO:

Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una perdida o daño en un activo de información.

ROUTER:

Un router (en español 'enrutador' o 'encaminador') es un dispositivo hardware o software de interconexión de redes de computadoras que opera en la capa tres (nivel de red) del modelo OSI. Este dispositivo interconecta segmentos de red o redes enteras. Hace pasar paquetes de datos entre redes tomando como base la información de la capa de red. El router toma decisiones lógicas con respecto a la mejor ruta para el envío de datos a través de una red interconectada y luego dirige los paquetes hacia el segmento y el puerto de salida adecuados. Sus decisiones se basan en diversos parámetros. Una de las más importantes es decidir la dirección de la red hacia la que va destinado el paquete (En el caso del protocolo IP esta sería la dirección IP). Otras decisiones son la carga de tráfico de red en las distintas interfaces de red del router y establecer la velocidad de cada uno de ellos, dependiendo del protocolo que se utilice.

SAMURAI:

Son lo más parecido a una amenaza pura. Sabe lo que busca, donde encontrarlo y cómo lograrlo. Hace su trabajo por encargo y a cambio de dinero, no tienen conciencia de comunidad y no forman parte de los clanes reconocidos por los hackers.

SGSI:

Sistema de gestión de la seguridad de la información. Sistema de gestión que establece, implementa, monitorea, monitorea, revisa, mantiene y mejora la seguridad de la información, previo análisis de riesgos.

SNIFFER:

Es un programa que monitoriza los paquetes de datos que circulan por una red. Mas claramente, todo lo que circula por la red va en 'paquetes de datos' que el sniffer chequea en busca de información referente unas cadenas prefijadas por el que ha instalado el programa.

SHELL:

Este concepto puede dar lugar a confusión ya que una shell en un sistema unix es un programa que interactúa entre el kernel y el usuario mientras que en nuestros ambientes significa el conjunto de login y password.... es decir que si alguien dice que cambia shells ya sabéis a lo que se refiere no?

SIP:

Session Initiation Protocol (SIP o Protocolo de Inicialización de Sesiones) es un protocolo desarrollado por el IETF MMUSIC Working Group con la intención de ser el estándar para la iniciación, modificación y finalización de sesiones interactivas de usuario donde intervienen elementos multimedia como el video, voz, mensajería instantánea, juegos online y realidad virtual. En Noviembre del año 2000, SIP fue aceptado como el protocolo de señalización de 3GPP y elemento permanente de la arquitectura IMS (IP Multimedia Subsystem). SIP es uno de los protocolos de señalización para voz sobre IP, acompañado por H.323.

SEGU-INFO.COM.AR

SMB/CIFS:

Server Message Block. Protocolo de red que permite compartir archivos e impresoras (entre otras cosas) entre nodos de una red. Es utilizado principalmente en ordenadores con Microsoft Windows. SMB fue originalmente inventado por IBM, pero la versión más común hoy en día es la modificada ampliamente por Microsoft. Microsoft renombró SMB a Common Internet File System (CIFS) en 1998 y añadió más características, que incluyen soporte para enlaces simbólicos, enlaces duros (hard links), y mayores tamaños de archivo. Hay características en la implementación de SMB de Microsoft que no son parte del protocolo SMB original. También existe Samba, que es una implementación libre del protocolo SMB con las extensiones de Microsoft. Funciona sobre sistemas operativos GNU/Linux y en otros UNIX.

SMURFING:

Técnica para que en un Broadcast todos los nodos de la red respondan a un victima (IP) particular. Contestaran aquellos que tengan habilitado contestar a peticiones destinadas a Broadcast.

SMTP:

Simple Mail Transfer Protocol (SMTP), o protocolo simple de transferencia de correo. Protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras o distintos dispositivos (PDA's, teléfonos móviles, etc.). Está definido en el RFC 2821 y es un estándar oficial de Internet

SNMP:

El Protocolo Simple de Administración de Red o SNMP es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Es parte de la familia de protocolos TCP/IP. SNMP permite a los administradores supervisar el desempeño de la red, buscar y resolver sus problemas, y planear su crecimiento. Las versiones de SNMP más utilizadas son dos: SNMP versión 1 (SNMPv1) y SNMP versión 2 (SNMPv2). Ambas versiones tienen un número de características en común, pero SNMPv2 ofrece mejoras, como por ejemplo, operaciones adicionales. SNMP en su última versión (SNMPv3) posee cambios significativos con relación a sus predecesores, sobre todo en aspectos de seguridad, sin embargo no ha sido mayoritariamente aceptado en la industria.

SNIFFING:

La interceptación lógica de datos. Un sniffer, o más concretamente, un sniffer de paquetes, se define como una pieza de software o hardware que se conecta a una red informática y supervisa todo el tráfico que pasa por el cable. Al igual que los dispositivos de intervención de teléfonos que usan las autoridades para escuchar conversaciones de otras personas, un programa de sniffing permite a alguien escuchar las conversaciones entre ordenadores que fluyen por las redes.

Las conversaciones entre ordenadores consisten en, aparentemente, datos binarios aleatorios. Por lo tanto, los programas de intervención necesitan disponer de una característica denominada "análisis de protocolo", la cual permite decodificar el tráfico enviado y darle sentido para hacerlo de "alguna manera" legible.

El arte de sniffing tiene una gran ventaja sobre las intervenciones telefónicas: la mayoría de las redes aún usan topologías de red compartidas. Esto quiere decir que no es necesario que el ordenador al cual se quiera monitorizar deba estar situado en las proximidades, simplemente si está conectado al mismo cable será susceptible de ser intervenido. Esto se conoce como un sniffer en modo promiscuo.

En cambio, la tecnología compartida (usando hubs) está rápidamente desplazándose a tecnología conmutada (switches), donde estas tácticas ya no son posibles. Aún así, existen varias técnicas de sniffing usadas en redes conmutadas que serán analizadas en futuros artículos y que pueden servir para saber si sus datos viajan de una manera segura.

SEGU-INFO.COM.AR

Mientras un administrador de redes puede emplear mucho tiempo en conseguir que su red sea difícil de ser atacada mediante sniffers utilizando firewalls, switches, detectores de modo promiscuo, etc., lo cierto es que la mejor forma de protegerse ante estos ataques es la de encriptar el tráfico de red.

Algunas técnicas son las siguientes:

Secure Sockets Layer (SSL): está presente en todos los navegadores Web populares así como en los servidores HTTP más conocidos. Su ventajas ya han sido discutidas en numerosos artículos, pero para resumir diremos que permite una navegación encriptada no vulnerable (aunque alguien dijo que nada es invulnerable, y de hecho ya existen algunas utilidades para espiar tráfico SSL) a los sniffers.

Por ello, este tipo de seguridad es utilizada en Internet para transmitir información privada de los usuarios, como por ejemplo el número de la tarjeta de crédito.

PGP y S/MIME: El correo puede ser interceptado de muchas formas alternativas. Tenga en cuenta que un correo electrónico necesita, para llegar a su destino, atravesar distintos servidores de red, firewalls y routers. Por ello, la posibilidad de que alguien pueda leer el correo es muy elevada si se envía sin ningún sistema de encriptación.

Los métodos más comunes para realizar esto son PGP (Pretty Good Privacy) y S/MIME (Secure MIME). PGP puede usarse como un añadido a diferentes productos y S/MIME está incluido en la mayoría de los nuevos gestores de correo como Outlook o Netscape, aunque dentro de Internet puede encontrar ambos productos para implementarlos en sus clientes (en páginas dedicadas a encriptación).

Secure Shell (Ssh): se ha convertido en el estándar de facto para acceder remotamente a servidores UNIX a través de Internet. Si aún sigue utilizando el protocolo telnet, debería reemplazarlo inmediatamente con este servicio. El producto fue diseñado por una compañía finlandesa pero se puede encontrar en muchas implementaciones freeware.

Virtual Private Networks (VPN): las redes virtuales privadas envían la información encriptada desde una red local a otra lejana geográficamente a través de Internet. En cambio, si un hacker interviene uno de los nodos iniciales de una red VPN podría aún capturar el tráfico. Sin duda es un sistema bastante fiable que es usado por la mayoría de las empresas que permiten el trabajo desde casa.

Componentes de un sniffer de paquetes:

El hardware: La mayoría de productos funcionan sobre adaptadores de red estándar, aunque algunos requieren hardware especial. Con analizadores industriales especializados, es posible comprobar fallos como errores de CRC, problemas de voltaje, errores de negociación, etc.

Driver de captura: Esta es la parte más importante. Captura el tráfico de red del cable, filtra un contenido específico definido por el usuario, y entonces almacena el resultado en un buffer.

Buffer: Una vez los paquetes son capturados de la red, estos se almacenan en un buffer. Existen un par de modos de captura: hasta que el buffer se llene, o usar un buffer rotatorio (o del tipo Round Robin) donde los nuevos datos sobrescriben los más antiguos. Algunos productos como BlackICE Sentir IDS de Internet Security Systems pueden mantener un buffer rotativo de captura en disco capaz de operar a 100 mbps. Esto permite tener cientos de GB de buffer en lugar de estar limitado por la cantidad de memoria del equipo.

Análisis en tiempo real: Esta característica realiza algunos análisis a nivel de bits de los paquetes que atraviesan el cable. Esto permite encontrar fallos de eficiencia en la red mientras continua capturando. Algunos vendedores han extendido estas funcionalidades en algunos de sus productos para pasar a ser IDS, aunque aún queda mucho trabajo por hacer en las herramientas de detección de hackers.

Decodificación: Como ya se ha discutido en el artículo, esta característica transforma los datos binarios a un formato entendible para su posterior análisis.

Editar paquetes (transmitir): Algunos productos (los menos) contienen características

SEGU-INFO.COM.AR

de editar los paquetes en la propia red y enviarlos de nuevo a ella. Es decir pueden generar paquetes personalizados usados con fines muy definidos. Algunos hackers usan estas herramientas para realizar ataques man-in-the-middle mediante las cuales intervienen un tráfico y suplantan la identidad original del individuo (puede ser temible).

¿Qué es una dirección MAC?

Debido a que numerosas máquinas pueden tener acceso a un mismo segmento de una red ethernet, cada una de ellas debe disponer de un identificador único.

Esto se lleva a cabo usando un número de 12 dígitos representado normalmente en formato hexadecimal, o lo que es igual, un número de 48 bits.

7 Las siglas MAC hacen referencia a Media Access Control (Control de Acceso del Medio), y es básicamente la dirección Ethernet de un adaptador en concreto. Los primeros 24 bits del número MAC hacen referencia al fabricante de la tarjeta de red, y los siguientes 24 bits representan una tarjeta única asignada por el fabricante. La identificación del fabricante se llama OUI (Organizationally Unique Identifier). De esta forma se asegura que no existan dos tarjetas de red con las mismas direcciones MAC.

SNOOPING:

Los ataques de esta categoría tienen el mismo objetivo que el sniffing, obtener la información sin modificarla. Sin embargo los métodos son diferentes. Además de interceptar el tráfico de red, el atacante ingresa a los documentos, mensajes de e-mail y otra información guardada, realizando en la mayoría de los casos un downloading de esa información a su propia computadora.

El Snooping puede ser realizado por simple curiosidad, pero también es realizado con fines de espionaje y robo de información o software. Los casos mas resonantes de este tipo de ataques fueron : el robo de un archivo con mas de 1700 números de tarjetas de crédito desde una compañía de música mundialmente famosa, y la difusión ilegal de reportes oficiales reservados de las Naciones Unidas, acerca de la violación de derechos humanos en algunos países europeos en estado de guerra.

SPOOFING:

Por spoofing se conoce a la creación de tramas TCP/IP utilizando una dirección IP falseada; la idea de este ataque - al menos la idea - es muy sencilla: desde su equipo, un pirata simula la identidad de otra máquina de la red para conseguir acceso a recursos de un tercer sistema que ha establecido algún tipo de confianza basada en el nombre o la dirección IP del host suplantado.

Esta técnica es utilizada para actuar en nombre de otros usuarios, usualmente para realizar tareas de snoofing o tampering. Una forma común de spoofing, es conseguir el nombre y password de un usuario legítimo para, una vez ingresado al sistema, tomar acciones en nombre de él, como puede ser el envío de falsos e-mails.

SOLARIS:
Sistema operativo de Sun.

SOX:

Ley de reforma de la contabilidad de compañías públicas y protección de los inversores aplicada en EEUU desde 2002. El objetivo es establecer un sistema de supervisión adecuada a las empresas y filiales que cotizan en las bolsas de valores de ese país.

SSH:

SSH (Secure SHell) es el nombre de un protocolo y del programa que lo implementa, y

SEGU-INFO.COM.AR

sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos, y también puede redirigir el tráfico de X para poder ejecutar programas gráficos si tenemos un Servidor X arrancado.

Además de la conexión a otras máquinas, SSH nos permite copiar datos de forma segura (tanto ficheros sueltos como simular sesiones FTP cifradas), gestionar claves RSA para no escribir claves al conectar a las máquinas y pasar los datos de cualquier otra aplicación por un canal seguro tunelizado mediante SSH.

SSL:

SSL proporciona autentificación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía. Habitualmente, sólo el servidor es autentificado (es decir, se garantiza su identidad) mientras que el cliente se mantiene sin autentificar; la autentificación mutua requiere un despliegue de infraestructura de claves públicas (o PKI) para los clientes. Los protocolos permiten a las aplicaciones cliente-servidor comunicarse de una forma diseñada para prevenir escuchas (eavesdropping), la falsificación de la identidad del remitente y mantener la integridad del mensaje.

SSL implica una serie de fases básicas:

Negociar entre las partes el algoritmo que se usará en la comunicación

Intercambio de claves públicas y autenticación basada en certificados digitales

Encriptación del tráfico basado en cifrado simétrico

Durante la primera fase, el cliente y el servidor negocian qué algoritmos criptográficos se van a usar. Las implementaciones actuales proporcionan las siguientes opciones:

Para criptografía de clave pública: RSA, Diffie-Hellman, DSA (Digital Signature Algorithm) o Fortezza; Para cifrado simétrico: RC2, RC4, IDEA (International Data Encryption Algorithm), DES (Data Encryption Standard), Triple DES o AES (Advanced Encryption Standard);

Con funciones hash: MD5 o de la familia SHA.

SWITCH:

Un switch (en castellano "conmutador") es un dispositivo de interconexión de redes de computadoras que opera en la capa 2 (nivel de enlace de datos) del modelo OSI (Open Systems Interconection). Un switch interconecta dos o más segmentos de red, funcionando de manera similar a los puentes (bridges), pasando datos de un segmento a otro, de acuerdo con la dirección MAC de destino de los datagramas en la red.

Un switch en el centro de una red en estrella. Los switches se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola. Al igual que los bridges, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las LANs (Local Area Network-Red de Área Local).

Tabla de contenidos:

Interconexión de switches y bridges

Los bridges y switches pueden ser conectados unos a los otros, pero existe una regla

SEGU-INFO.COM.AR

que dice que sólo puede existir un único camino entre dos puntos de la red. En caso de que no se siga esta regla, se forma un bucle en la red, lo que tiene como resultado la transmisión infinita de datagramas de una red a otra.

Sin embargo, esos dispositivos utilizan el algoritmo de spanning tree para evitar bucles, haciendo la transmisión de datos de forma segura.

Introducción al funcionamiento de los conmutadores

Conexiones en un switch Ethernet. Los conmutadores poseen la capacidad de aprender y almacenar las direcciones de red de nivel 2 (direcciones MAC) de los dispositivos alcanzables a través de cada uno de sus puertos. Por ejemplo, un equipo conectado directamente a un puerto de un conmutador provoca que el conmutador almacene su dirección MAC. Esto permite que, a diferencia de los concentradores o hubs, la información dirigida a un dispositivo se dirija únicamente desde el puerto origen al puerto que permite alcanzar el dispositivo destino.

En el caso de conectar dos conmutadores o un conmutador y un concentrador, cada conmutador aprenderá las direcciones MAC de los dispositivos accesibles por sus puertos, por tanto en el puerto de interconexión se almacenan las MAC de los dispositivos del otro conmutador.

Bucles de red e inundaciones de tráfico

Como anteriormente se comentaba, uno de los puntos críticos de estos equipos son los bucles (ciclos) que consisten en habilitar dos caminos diferentes para llegar de un equipo a otro a través de un conjunto de conmutadores. Los bucles se producen porque los conmutadores que detectan que un dispositivo es accesible a través de dos puertos emiten la trama por ambos. Al llegar esta trama al conmutador siguiente, este vuelve a enviar la trama por los puertos que permiten alcanzar el equipo. Este proceso provoca que cada trama se multiplique de forma exponencial, llegando a producir las denominadas inundaciones de la red, provocando en consecuencia el fallo o caída de las comunicaciones.

Como se ha comentado se emplea el protocolo spanning tree para evitar este tipo de fallos.

Conmutadores de nivel 3

Aunque los conmutadores o switches son los elementos que fundamentalmente se encargan de encaminar las tramas de nivel 2 entre los diferentes puertos, existen los denominados conmutadores de nivel 3 o superior, que permiten crear en un mismo dispositivo múltiples redes de nivel 2 (ver VLANs) y encaminar los paquetes (de nivel 3) entre las redes, realizado por tanto las funciones de encaminamiento o routing (ver router).

TCP/IP:

La Familia de protocolos de internet es un conjunto de protocolos de red en la que se basa Internet y que permiten la transmisión de datos entre redes de computadoras. En ocasiones se la denomina conjunto de protocolos TCP/IP, en referencia a los dos protocolos más importantes que la componen: Protocolo de Control de Transmisión (TCP) y Protocolo de Internet (IP), que fueron los dos primeros en definirse, y que son los más utilizados de la familia. Existen tantos protocolos en este conjunto que llegan a ser más de 100 diferentes, entre ellos se encuentra el popular HTTP (HyperText Transfer Protocol), que es el que se utiliza para acceder a las páginas web, además de otros como el ARP (Address Resolution Protocol) para la resolución de direcciones, el FTP (File Transfer Protocol) para transferencia de archivos, y el SMTP (Simple Mail Transfer Protocol) y el POP (Post Office Protocol) para correo electrónico, TELNET para acceder a equipos remotos, entre otros.

El TCP/IP es la base de Internet, y sirve para enlazar computadoras que utilizan diferentes sistemas operativos, incluyendo PC, minicomputadoras y computadoras centrales sobre redes de área local (LAN) y área extensa (WAN). TCP/IP fue desarrollado y demostrado por primera vez en 1972 por el departamento de defensa de los Estados Unidos, ejecutándolo en ARPANET, una red de área extensa del departamento de defensa.

SEGU-INFO.COM.AR

TELNET:

Telnet (TELecommunication NETwork) es el nombre de un protocolo de red (y del programa informático que implementa el cliente), que sirve para acceder mediante una red a otra máquina, para manejarla como si estuviéramos sentados delante de ella. Para que la conexión funcione, como en todos los servicios de Internet, la máquina a la que se acceda debe tener un programa especial que reciba y gestione las conexiones. El puerto que se utiliza generalmente es el 23.

TEST DE INTRUSIÓN:

El Test de Intrusión se centra en evaluar la seguridad de los sistemas de protección perimetral de una empresa así como los diferentes sistemas que están accesibles desde Internet (routers exteriores, firewall exterior, servidores web, de correo, de noticias, etc). Intentando penetrar en ellos y de esta forma alcanzar zonas de la red de una empresa como puede ser la red interna o la DMZ.

TFTP:

TFTP son las siglas de Trivial File Transfer Protocol (Protocolo de transferencia de archivos trivial).

Es un protocolo de transferencia muy simple semejante a una versión básica de FTP. TFTP a menudo se utiliza para transferir pequeños archivos entre ordenadores en una red, como cuando un terminal X Window o cualquier otro cliente ligero arrancan desde un servidor de red.

Algunos detalles del TFTP:

Utiliza UDP (puerto 69) como protocolo de transporte (a diferencia de FTP que utiliza el puerto 21 TCP).

No puede listar el contenido de los directorios.

No existen mecanismos de autentificación o encriptación.

Se utiliza para leer o escribir archivos de un servidor remoto.

Soporta tres modos diferentes de transferencia, "netascii", "octet" y "mail", de los que los dos primeros corresponden a los modos "ascii" e "imagen" (binario) del protocolo FTP.

Detalles de una sesión TFTP

Ya que TFTP utiliza UDP, no hay una definición formal de sesión, cliente y servidor. Sin embargo, cada archivo transferido vía TFTP constituye un intercambio independiente de paquetes, y existe una relación cliente-servidor informal entre la máquina que inicia la comunicación y la que responde.

La máquina A, que inicia la comunicación, envía un paquete RRQ (read request/petición de lectura) o WRQ (write request/petición de escritura) a la máquina B, conteniendo el nombre del archivo y el modo de transferencia.

B responde con un paquete ACK (acknowledgement/confirmación), que también sirve para informar a A del puerto de la máquina B al que tendrá que enviar los paquetes restantes.

La máquina origen envía paquetes de datos numerados a la máquina destino, todos excepto el último conteniendo 512 bytes de datos. La máquina destino responde con paquetes ACK numerados para todos los paquetes de datos.

El paquete de datos final debe contener menos de 512 bytes de datos para indicar que es el último. Si el tamaño del archivo transferido es un múltiplo exacto de 512 bytes, el

SEGU-INFO.COM.AR

origen envía un paquete final que contiene 0 bytes de datos.

TLS:

Secure Sockets Layer (SSL) y Transport Layer Security (TLS) -Seguridad de la Capa de Transporte-, su sucesor, son protocolos criptográficos que proporcionan comunicaciones seguras en Internet. Existen pequeñas diferencias entre SSL 3.0 y TLS 1.0, pero el protocolo permanece sustancialmente igual. El término "SSL" según se usa aquí, se aplica a ambos protocolos a menos que el contexto indique lo contrario.

TOKEN DE ACCESO:

Es una estructura de datos que contiene información de autorización para un usuario o un grupo. Un sistema utiliza un token de acceso para controlar el acceso a objetos seguros y para controlar la habilidad de un usuario para llevar a cabo varias operaciones relativas al sistema en una terminal.

TRACEAR:
Seguir la pista a través de la red a una información o de una persona.

TRASHING ("Basureo"):

Obtienen información en cubos de basura, tal como números de tarjetas de crédito, contraseñas, directorios o recibos.

TROYANO:
Programa que se queda residente en un sistema y que ha sido desarrollado para obtener algún tipo de información. Por ejemplo la función del troyano es ejecutarse al inicio del sistema víctima y luego enviar información de un archivo de /etc/passwd a una determinada IP que seria la del que coloca el troyano, paro la función principal de este programa es que el troyano toma el control de la máquina víctima haciéndola totalmente vulnerable.

UDP:
User Datagram Protocol (UDP) es un protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera. Tampoco tiene confirmación, ni control de flujo, por lo que los paquetes pueden adelantarse unos a otros; y tampoco se sabe si ha llegado correctamente, ya que no hay confirmación de entrega o de recepción. Su uso principal es para protocolos como DHCP, BOOTP, DNS y demás protocolos en los que el intercambio de paquetes de la conexión/desconexión son mayores, o no son rentables con respecto a la información transmitida, así como para la transmisión de audio y vídeo en tiempo real, donde no es posible realizar retransmisiones por los estrictos requisitos de retardo que se tiene en estos casos.

En la familia de protocolos de Internet UDP proporciona una sencilla interfaz entre la capa de red y la capa de aplicación. UDP no otorga garantías para la entrega de sus mensajes y el origen UDP no retiene estados de los mensajes UDP que han sido enviados a la red. UDP sólo añade multiplexado de aplicación y suma de verificación de la cabecera y payload. Cualquier tipo de garantías para la transmisión de la información, deben ser implementadas en capas superiores.

UNIX:
Familia de sistemas operativos que engloba a Sun OS, Solaris, irix, etc.

VMS:
Sistema operativo.

SEGU-INFO.COM.AR

VPN:

La Red Privada Virtual (RPV), en inglés Virtual Private Network (VPN), es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet son lo mejor que se ha implementado.

Ejemplos comunes son, la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, como por ejemplo un hotel. Todo ello utilizando la infraestructura de Internet.

Para hacerlo posible de manera segura es necesario proporcionar los medios para garantizar la autenticación, integridad y confidencialidad de toda la comunicación:

Autenticación y autorización: ¿Quién está del otro lado? Usuario/equipo y qué nivel de acceso debe tener.

Integridad: La garantía de que los datos enviados no han sido alterados. Para ello se utiliza funciones de Hash. Los algoritmos de hash más comunes son los Message Digest (MD2 y MD5) y el Secure Hash Algorithm (SHA).

Confidencialidad: Dado que los datos viajan a través de un medio potencialmente hostil como Internet, los mismos son susceptibles de intercepción, por lo que es fundamental el cifrado de los mismos. De este modo, la información no debe poder ser interpretada por nadie más que los destinatarios de la misma. Se hace uso de algoritmos de cifrado como Data Encryption Standard (DES), Triple DES (3DES) y Advanced Encryption Standard (AES).

No repudio: es decir, un mensaje tiene que ir firmado, y el que lo firma no puede negar que el mensaje lo envió él.

VIRUS:

Es un programa que se reproduce a si mismo y que muy posiblemente ataca a otros programas. Puede crear copias de si mismo y suele dañar archivos del sistema o realizar modificaciones en el mismo, puede cambiar o disminuir la capacidad de un sistema disminuyendo la memoria útil o el espacio libre.

VULNERABILIDAD:

Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo de la compañía.

WANNABER:

Desea ser hacker pero estos consideran que su coeficiente no da para tal fin. A pesar de su actitud positiva difícilmente consiga avanzar en sus propósitos.

WAR DIALER:

Estos son programas (también se podría hacer a mano, pero es muy pesado) que realizan llamadas telefónicas en busca de módem. Sirve para buscar maquinas sin hacerlo a través de Internet. Estas maquinas suelen ser muy interesantes ya que no reciben tantos ataques y a veces hay suerte y no están tan cerradas.

WORM O GUSANO:

Un gusano es un virus informático que tiene la propiedad de duplicarse a sí mismo. Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario.

SEGU-INFO.COM.AR

A diferencia de un virus, un gusano no precisa alterar los archivos de programas, sino que reside en la memoria y se duplica a sí mismo. Los gusanos siempre dañan la red (aunque sea simplemente consumiendo ancho de banda), mientras que los virus siempre infectan o corropen los archivos de la computadora que atacan.

Es algo usual detectar la presencia de gusanos en un sistema cuando, debido a su incontrolada replicación, los recursos del sistema se consumen hasta el punto de que las tareas ordinarias del mismo son excesivamente lentas o simplemente no pueden ejecutarse.

Los gusanos se basan en una red de computadoras para enviar copias de sí mismo a otros nodos (es decir, a otras terminales en la red) y es capaz de llevar esto a cabo sin intervención del usuario.

WINDOWS:
Sistema operativo de Microsoft.

ZAP:
Zap es un programa que se usa para borrar las huellas en un sistema. Debido a lo famoso que se ha hecho muchos programas que desarrollan estas funciones se les llama zappers.

SEGU-INFO.COM.AR