DEPARTAMENTO DE
INGENIERÍA
INFORMÁTICA
UNIVERSIDAD DE SANTIAGO DE CHILE

Fundamentos de ciberseguridad

Seguridad en las operaciones

Profesor

Mg. Juan Ignacio Iturbe A.

Introducción

- El profesional de la seguridad debe conocer:
  - que debe proteger,
  - los privilegios que deben ser restringidos,
  - los mecanismos de control disponibles,
  - el abuso potencial del acceso
  - Los controles apropiados
  - los principios y las buenas practicas

Introducción

- A continuación se revisará:
  - Gestión administrativa y controles
  - Conceptos de control de las operaciones y gestión
  - Amenazas a la seguridad y contramedidas

Gestión administrativa y controles

- Una organización necesita políticas y procedimientos claros y documentados.
- Hay numerosas mejores prácticas para proteger el negocio y sus importantes activos de información.
- Estas mejores prácticas tienen que ver con como la gente –no la tecnología- trabaja en conjunto para soportar el negocio.

Requerimientos y calificación para para el trabajo

- Antes de colocar cualquier anuncio de trabajo, se tiene que asegurar:
  - Que la posición vacante se encuentra claramente documentada
  - Contiene una completa descripción de los requerimientos del trabajo
  - Calificaciones correspondientes
  - El alcance de las responsabilidades y autoridad.

Roles y responsabilidades

Rol en la organización	Responsabilidades base
Analista de sistema	Diseña flujo de datos para los sistemas basados en requerimientos operacionales y de los usuarios
Programador de aplicaciones	Desarrolla y mantiene software de producción
Mesa de ayuda/Soporte	Resuelve incidentes y problemas operacionales o técnicos del usuario final o de sistema.
Ingeniero TI	Desarrolla el día a día de los deberes operacionales en los sistemas y aplicaciones
Administrador de base de datos	Crea nuevas tablas de base de datos y mantiene las base de datos
Administrador de red	Instala y mantiene las LANs/WANs
Administrador de seguridad	Define, configura, y mantiene los mecanismos de protección de la organización.


Increased cybersecurity responsibility and expertise
Cybersecurity Professionals
CISO, Director of Cybersecurity, cybersecurity team
Ensure implementation and management of security controls
Maintain current certifications
Senior IT Executives
CIO, VP of IT, IT Director, etc.
Ensure adherence to security and acceptable use policies
IT Operations
IT managers, directory server team
Require password resets every quarter
Ensure linkage with directory server
Maintain application whitelists
Restrict local device admin rights
Enterprise Administrators
System administrators, middle managers, program managers
Minimize assignment of admin rights
Review and update admin roster every quarter
Remove admin rights immediate when no longer needed
Local Administrators
Front line supervisors, junior managers, project managers
Provide access to authorized employees only
Review and update access every quarter
Remove access immediately when no longer needed
Use authorized backup only
Everyone
Front line employees, support staff, new hires, all managers and executives
Use strong, work-specific passwords
Don't open unknown attachments
Don't plug in unknown devices
Don't click on unknown links
Report suspicious activity
Layers of additional tasks

Requerimientos y calificación para para el trabajo

- Esto ayuda a la organización en muchas razones:
  - El encargado de contratación conoce exactamente que habilidades requiere un cierto trabajo.
  - El gerente de recursos humanos puede tener una visión de lo que se requiere de los postulantes al trabajo.
  - Los candidatos potenciales pueden asegurar que están postulando solamente a trabajos que ellos se encuentran calificados.
  - Después que la organización llena la posición, la descripción de esta ayuda a reducir la confusión sobre que espera la organización del nuevo empleado y provee un criterio objetivo para evaluar su desempeño.

Verificación de antecedentes

- Se deben chequear los antecedentes del postulante.
- Este proceso ayuda a exponer cualquier candidato indeseable o no calificado.
- Por ejemplos:
  - Registro criminal
  - Historial de crédito
  - Historial de empleado
  - Educación
  - Certificaciones y licencias
  - Miembro de asociaciones

Separación (o segregación) de deberes y responsabilidades

- Asegura que un solo individuo no tiene la autoridad y control de un sistema ó proceso crítico. Con lo que:
  - Reduce las oportunidades para el fraude o abuso.
  - Reduce los errores
  - Reduce la dependencia a los individuos.

Separación (o segregación) de deberes y responsabilidades

- Ejemplos:
  - Un banco le da tres de los seis números de una combinación a un empleado y los otros tres a otro empleado para tener acceso a un recurso crítico.
  - Un administrador de sistema es el responsable de crear nuevas cuentas y permisos de acceso, es el administrador de seguridad quien verifica.
  - Un programador desarrolla el código fuente, pero un individuo separado es el responsable de las pruebas y validación y otro responsable es el encargado de cargar el código fuente en producción.

Rotación de trabajo (o deberes)

- Es otro efectivo control de seguridad, que le da varios beneficios a la organización:
  - Reduce la oportunidad de fraude o abuso.
    - La gente vacila en realizar periódicamente robos porque puede ser movida en cualquier momento.
    - La gente no trabaja el tiempo suficiente para coludirse.
  - Elimina puntos únicos de falla
  - Promociona el crecimiento profesional.
    - Oportunidades de entrenamiento cruzado
    - Reduce la monotonía y la fatiga.

Vacaciones mandatorias

- Empleados que realizan actividades ilegales o prohibidas son renuentes a alejarse de la oficina.
- Ayudan a la organización a descubrir potenciales fraudes o abusos y también:
  - Reduce el estrés individual y las oportunidades de equivocaciones y coerción por otros.
  - Descubrir procesos ineficiente .
  - Revela puntos únicos de falla
  - Promueve la rotación de trabajo.

Need-to-know

- Solamente la gente con una valida necesidad de conocer cierta información en orden de realizar su funciones debe tener el acceso.
- Un individuo debe tener también el apropiado nivel de autorización de seguridad para conceder el acceso.
- Este concepto esta relacionado estrechamente con el concepto de mínimo privilegio.

Mínimo privilegio

- El mínimo privilegio
  - es lo que la persona debe tener para que pueda **desarrollar una tarea**
  - o **el acceso a un dato** que es requerido para desarrollar sus tareas primarias.
- Por ejemplo,
  - darle a un usuario todos los permisos a una carpeta de red compartida, en vez de darle solamente lectura y modificación a un directorio específico. ¿Qué puede pasar?
- Una estrategia a adoptar es “deny all” y dar permisos específicos.

Monitoreo de usuario

- Monitorear las actividades de los usuarios de la organización, es una buena práctica de seguridad.
  - en especial de quienes tienen privilegios importantes
- Puede incluir,
  - Observación casual o directa
  - Análisis de logs
  - Inspección de discos duros de estaciones de trabajo.
  - Pruebas contra drogas aleatorio de acuerdo a la ley.
  - Revisión del log de llamadas, etc.

Monitoreo de usuario

- El monitoreo de usuario y sus propósitos debe estar escrito en el manual de políticas y/o reglamento interno.
- Los sistemas de información deben incluir una advertencia que las actividades pueden ser monitoreadas y su razón.
  - Ej, llamado a un call center

Termino de un empleo

- Empleados que violan un política de seguridad son sujetos de una acción disciplinaria que puede incluir su despido.
- Es vital bloquear o revocar el acceso local y remoto al empleado lo mas pronto posible,
  - especialmente cuando el usuario es despedido.
  - Un ex-empleado enojado puede traer serios peligros.

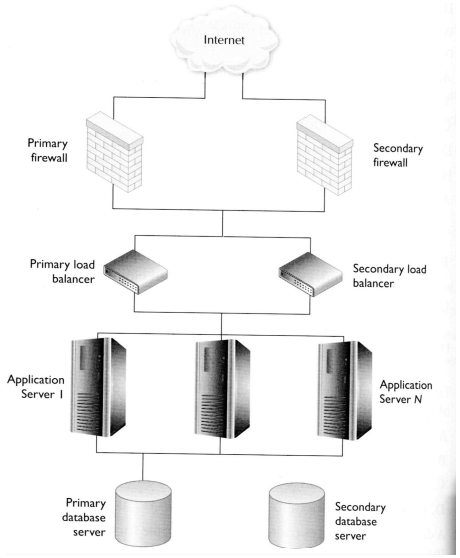
Conceptos de Seguridad en las operaciones

- El tema central en la Seguridad de las operaciones es proteger la confidencialidad, integridad y disponibilidad de los activos de información en el día a día.
- Para ello se debe:
  - Evitar los puntos únicos de falla.
  - Manejar la información sensible
  - Retener registros

Evitando puntos únicos de falla

- Un punto único de falla es una parte de un sistema, proceso o red que puede fallar y causar que todo el sistema se encuentre no disponible.
- Existen varias estrategias y soluciones para contrarrestar esto:
  - Grid computing
  - Alta disponibilidad (HA)
  - Clustering
  - Mirroring
  - RAID's
  - Virtualización
  - Etc.

Tarea: Averiguar sobre los distintos tipos de RAID, SAN, DAS, NAS



Caso práctico: Virtualización

- Dos servidores físicos:
  - *hostiando* múltiples servidores virtuales
  - comparten un *storage* común (por ejemplo una SAN).
- Si el servidor #1 falla,
  - todos los servidores virtuales en el servidor pueden ser "movidos" al servidor físico #2.

Caso práctico: Virtualización

- En un escenario alternativo,
  - Si un servidor virtual en el servidor físico #1 tiene un umbral de performance pre-definido (Como procesador, memoria o utilización de ancho de banda)
  - El servidor virtual puede ser “movido” automáticamente al servidor físico #2

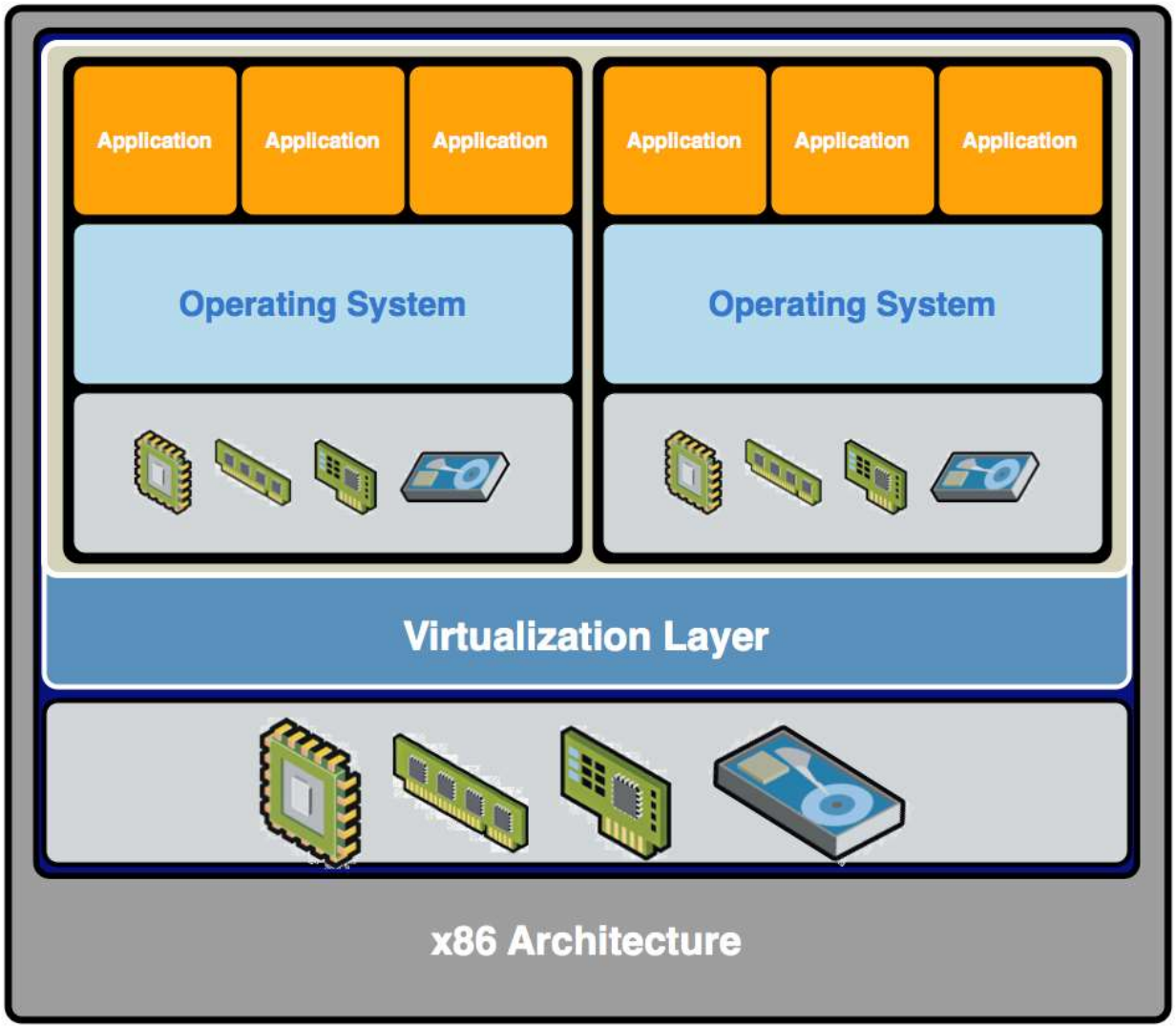


*Imagen obtenida de http://xamin.ir/ist/whatisxamin/#/step-1

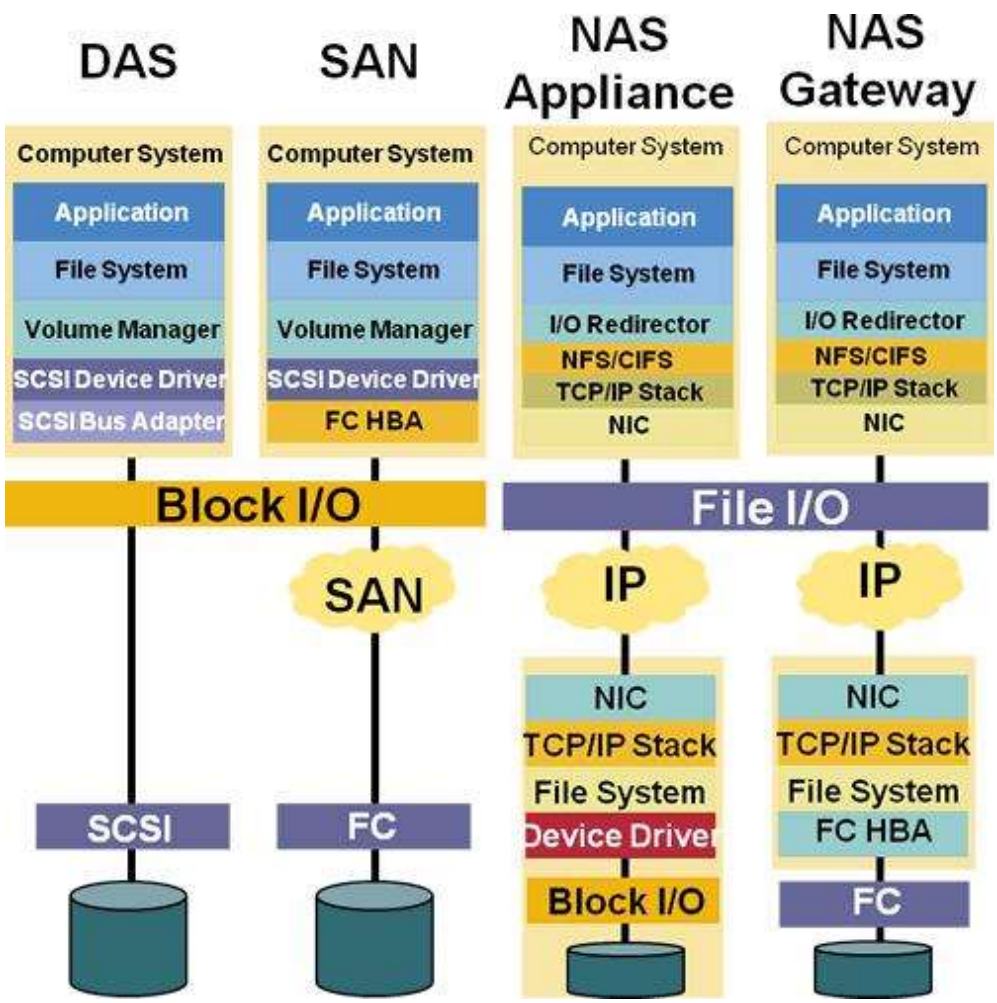


*Imagen sacada desde http://rm-rf.es/storage-diferencias-entre-nas-san-y-das/

Puntos únicos de falla

- En la realidad cualquier sistema, proceso o red tiene numerosos puntos únicos de falla.
- Un plan de seguridad efectivo identifica y elimina cada uno de ellos.
- Por ejemplo, a través de una tormenta de ideas (*brainstorming*) se pueden identificar muchos de estos puntos.

En la *brainstorming* …

- Sistemas:
  - ¿Los servidores tienen fuentes de poder redundantes y fans de enfriamiento?
  - ¿Los HDD están configurados para RAID?¿Los componentes son *hot-swap*?
  - ¿Los sistemas pueden y deben ser *clusterizados* o *virtualizados*?
  - ¿Los datos pueden ser replicados a otro sistema/locación en tiempo real?

En la *brainstorming* …

- Redes:
  - ¿Los *routers* y *firewalls* corren sobre fallas automáticamente?
  - ¿Pueden recuperarse desde la falla?
  - ¿Los *routers* tienen múltiples caminos disponibles para las redes destino?
  - ¿Tienes múltiples proveedores de servicios?
  - ¿Ellos comparten el mismo POPs (punto de presencia) de red?
  - ¿Qué pasa si la conexión a tú proveedor de comunicación es cortada?
  - ¿Los proveedores de comunicación comparten instalaciones entre sí?

En la *brainstorming* …

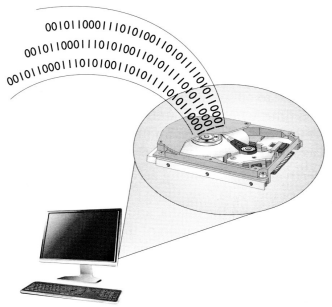
- Procesos:
  - ¿Tus políticas y prácticas de seguridad del personal crean puntos únicos de falla?
    - Quizás se realizo la separación de funciones y responsabilidades, pero no se estableció una correspondiente rotación de deberes y responsabilidades.
  - ¿Tienes un procesos de contingencia andando en caso que un sistema primario, procesos o persona no está disponible?

Manejando información sensible

- Información sensible como registros financieros, datos de empleados e información sobre los clientes debe ser:
  - claramente marcada,
  - adecuadamente manejada y almacenada
  - apropiadamente destruida de acuerdo a las políticas, estándares y procedimientos de la organización

Manejando información sensible

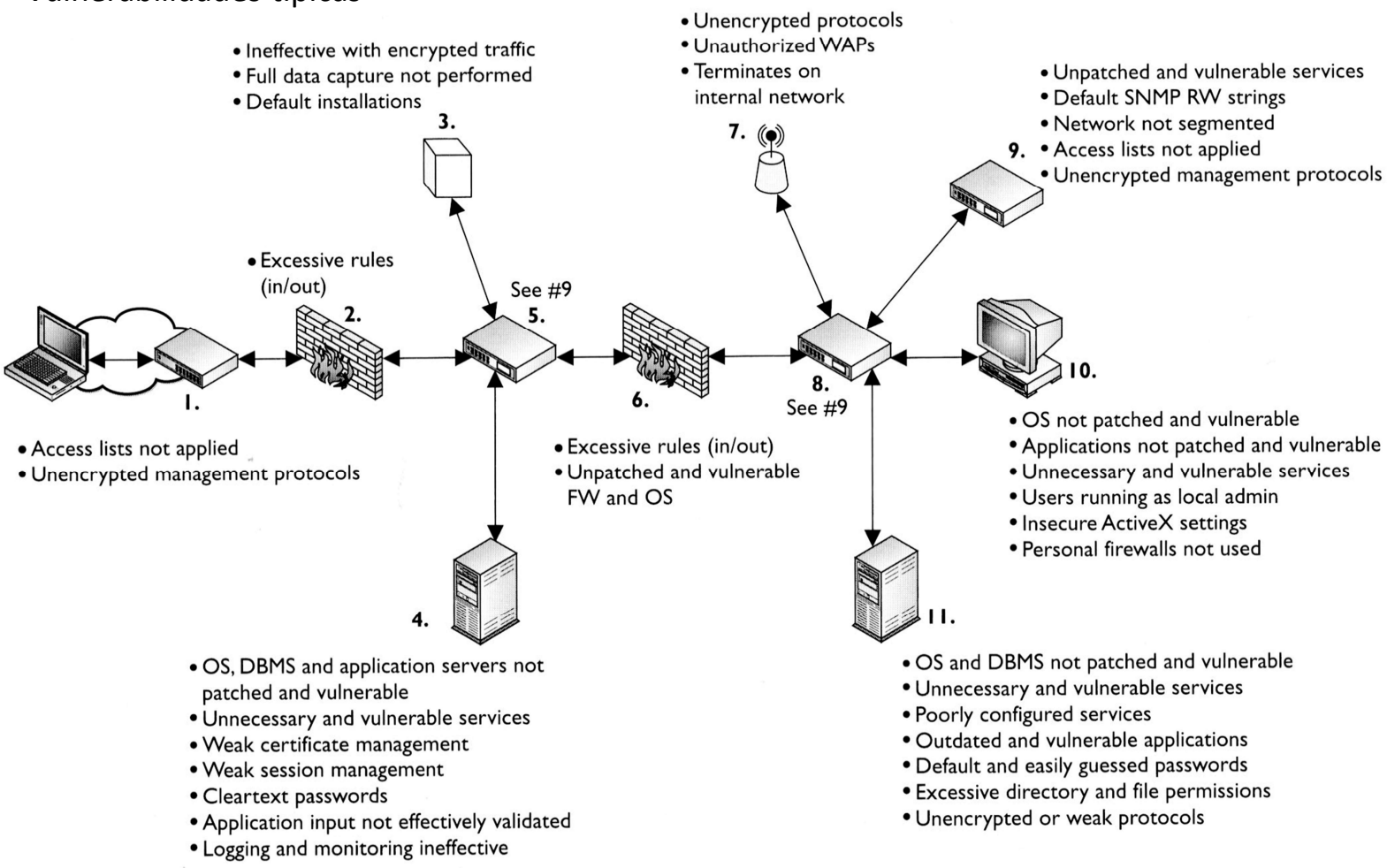
- Marcaje: Como la organización identifica información sensible. Ej: una marca puede ser “CONFIDENCIAL”.
- Manejo: Se detalla como los empleados pueden transportar, transmitir y usar la información.
- Almacenamiento y respaldo: Similar al manejo, deben haber procedimientos para almacenar y respaldar.
- Destrucción: Debe haber un procedimiento detallado sobre como destruir información sensible que puede estar previamente retenida, o guardada en un archivo electrónico



Amenazas y contramedidas

Amenaza	Contramedida
Errores y omisiones	Revisiones y proceso de control de calidad
Fraude	Sistema de detección de fraude (analiza transacciones y provee un lista de posibles). Revisión de roles y responsabilidades, para evitar la colusión
Hackers y Crackers	Firewalls, HIDS, NIDS, IPS, etc.
Espionaje industrial	Trazas de auditoría y control de acceso
Malware	Antivirus, antispyware
Sabotaje	Control de acceso estricto tanto lógico como físico.
Robo	Control de acceso físico
Perdida de soporte físico e infraestructura	Discutidas en seguridad física

Vulnerabilidades típicas



Controles de seguridad

- Varios tipos:
  - Controles preventivos
  - Controles detectivos
  - Controles correctivos
  - Controles automáticos
  - Controles manuales

Controles de operaciones

- Procesos y/o procedimientos que protegen las operaciones del negocio y la información:
  - Protección de recursos
  - Controles de entidad privilegiada
  - Controles de cambio
    - Gestión del cambio y configuración
  - Controles de medios
  - Controles administrativos
  - Recuperación confiable (*Trusted recovery*)

Protección de recursos

Recursos	Ejemplos que requieren protección
Hardware de comunicaciones y software	Routers, switchs, firewalls, balanceadores de carga, maquinas de fax, servidores VPN y todo el software que usan estos dispositivos
Computadores y sus sistemas de almacenamiento	Servidores corporativos, estaciones de trabajo, SAN, NAS, DAS, sistemas de almacenamiento y dispositivos de respaldos
Datos del negocio	Toda la información almacenada, datos financieros, ventas e información de marketing, personal e información de pagos, datos de clientes y proveedores, productos propietarios o datos de procesos e información de propiedad intelectual.
Datos del sistema	S.O., utilidades, Identificación de usuarios y archivos de password, trazas de auditorias y archivos de configuración
Medios de respaldo	Tapes, discos removibles, discos con sistemas replicados
Software	Código fuente, programas, herramientas, librerías, software externo, y otro software propietario.

Auditoría de seguridad y debido cuidado

- Auditoría es el proceso de examinar sistemas y/o procesos de negocio para asegurar que ellos son diseñados y usados adecuadamente.
- Las auditorías frecuentemente son realizadas por terceras partes, grupos autónomos de la organización.
- Los sistemas críticos deben ser continuamente auditados como dicte la regulación, contratos o requerimientos.
- El debido cuidado, requiere que la organización opere usando las mejores prácticas de negocio.

Trazas de auditoría

- También conocidos como logs de auditoría o simplemente logs.
- Son los registros auxiliares que son creados con los registros de transacciones y otros eventos. Estos son creados por
  - Obligar la *accountability* (dar cuenta de los actos).
  - Investigación
  - Reconstrucción de eventos
  - Identificación de problemas.
- Generalmente está compuesta por:
  - Fecha y hora (importante, sincronizar relojes, servidor NTP)
  - Quien
  - Donde
  - Detalles

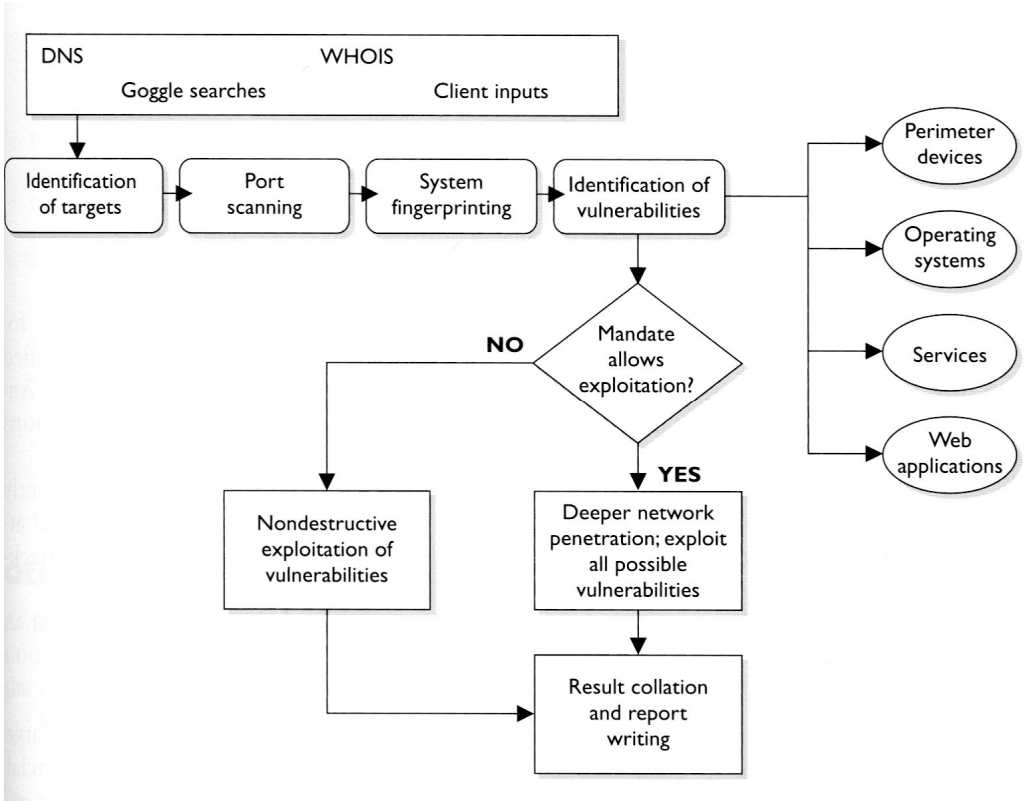
Monitoreo

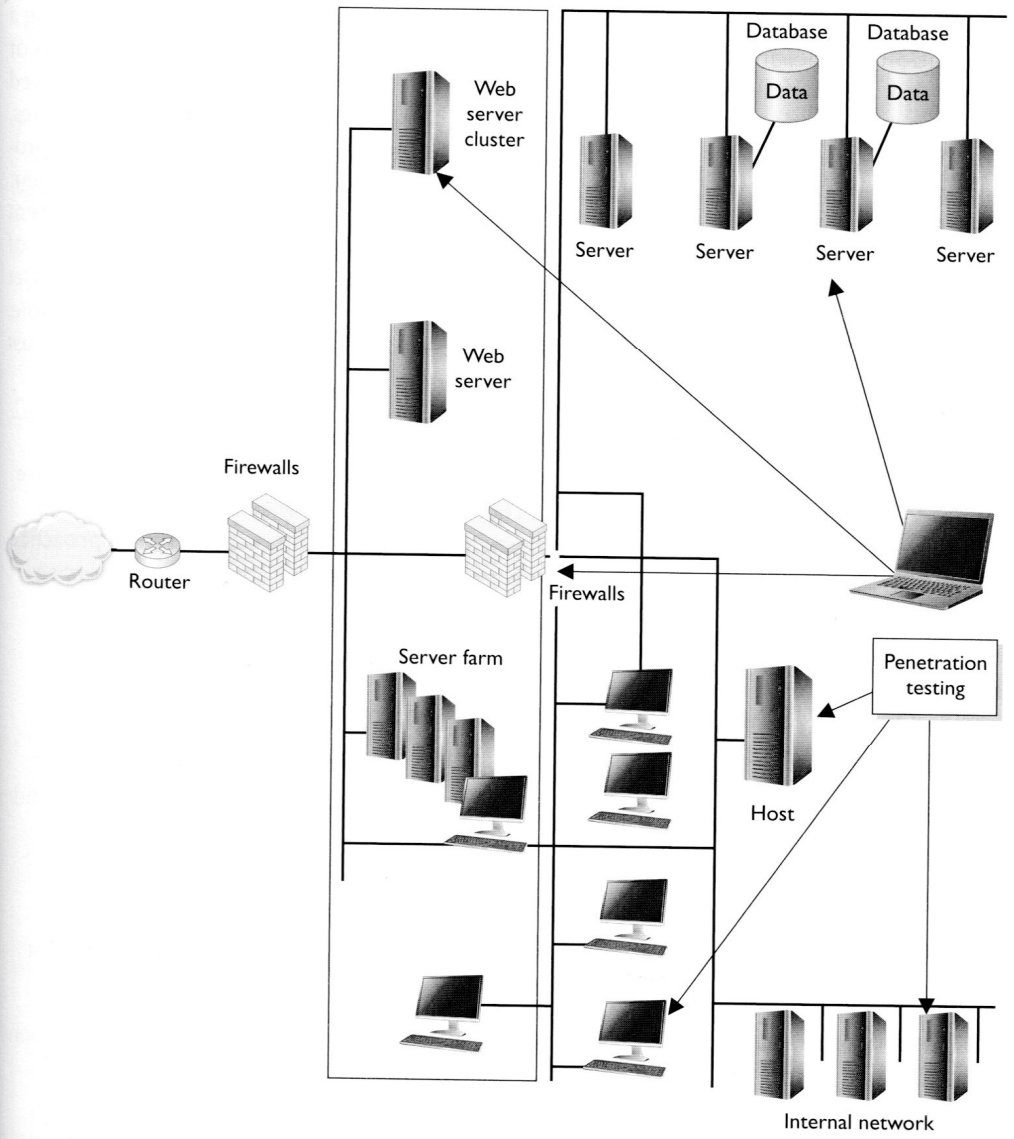
- Incorpora las siguientes actividades:
  - Test de penetración
  - Detección de intrusos
  - Análisis de Violaciones (*Clipping levels*)
  - *Keystroke monitoring*
  - Análisis de tráfico y tendencias
  - Monitoreo de la instalaciones

Monitoreo

- Test de penetración
  - Escáner de puertos
  - Escáner de vulnerabilidades
  - Sniffing de paquetes
  - War dialing
  - War driving
  - Monitoreo de RF
  - Revisión de basura
  - Shoulder surfing
  - Ingeniería social

Test de penetración





"El test de penetración es usado para probar que un atacante actualmente puede comprometer los sistemas"

Monitoreo

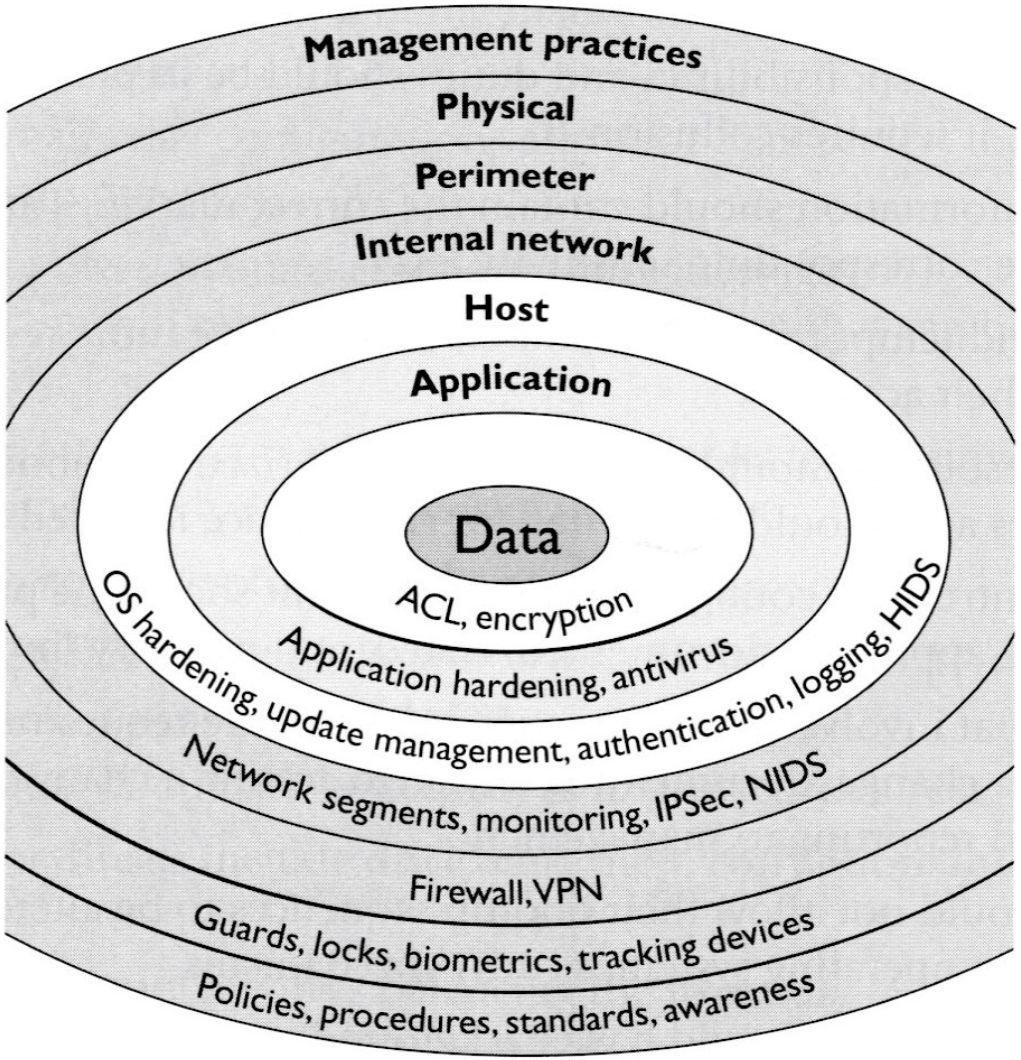
- Detección y prevención de intrusos
  - Por locación
    - Basada en red (NIDS)
    - Basada en host (HIDS)
  - Por método de clasificación:
    - Basado en firma
    - Basado en anomalías

Ejemplo firma snort:
alert tcp any 110 -> (content:
“filename=\”TOMOFONICA.TXT.vbs\”";\
nocase; msg: “Virus tomofonica”;)

alert tcp $EXTERNAL_NET any -> $HOME_NET any
/ (msg:”Escaneo ping con nmap”;flags:A;ack:0; /
reference:arachnids,28;classtype:attempted-recon;
sid:628;/ rev:1;)

Respondiendo a eventos

- Se requiere el siguiente planeamiento:
  - Personal de monitoreo
  - Respuesta inicial
  - Confirmación
  - Notificación
  - Escalamiento
  - Resolución
  - Reporte de evento
  - Revisión del evento
  - Violación de seguridad (análisis de causa raíz)


Management practices
Physical
Perimeter
Internal network
Host
Application
Data
ACL, encryption
Application hardening, antivirus
OS hardening, update management, authentication, logging, HIDS
Network segments, monitoring, IPSec, NIDS
Firewall, VPN
Guards, locks, biometrics, tracking devices
Policies, procedures, standards, awareness

En resumen…

Referencias

- CISSP, All in one sixth edition, Shon Harris
- CEH, Certified Ethical Hacker, All in one, Matt Walker