Gestión Activa de la seguridad

Seguridad activa

Medidas que pretenden prevenir posibles ataques.
Si se produce un ataque, se debe conocer primero cuál es el objetivo del atacante y qué método ha utilizado en el ataque. Tendremos que conocer las posibles vulnerabilidades de nuestro sistema y hacer lo posible para reducirlas o eliminarlas.

Riesgos Asociados a las personas

Algunos son:

- Atacantes usando la ingeniería social.
- Configuración incorrecta de usuarios, grupos, permisos, derechos, etc.
- Desconfiar el eliminar usuarios y cuentas que no son útiles.
- Errores de documentación.
- Etc.

El ataque informático

Procedimiento de análisis para un ataque informático:

- ¿Qué sistemas componen la red?
- ¿Qué vulnerabilidades tiene el sistema en red?
- Explotación de las vulnerabilidades detectadas.
- Inyección del payload.
- Ocultación o eliminación de rastros que prueban el ataque.

Tipos de ataque informáticos comunes

- Capturación de información.
- Detección de vulnerabilidades.
- Robo de información por interceptación de tráfico.
- Cifrado de información almacenada sobre clave atacante. Secuestro.
- Etc.

Herramientas para el ataque

- Escáneres de puertos. Detectan los servicios instalados en el sistema o en otro sistema remoto.
- Sniffer. Son dispositivos o apps que escuchan la red para capturar los paquetes de datos que circulan por ella.
- Exploits. Herramientas que buscan y explotan vulnerabilidades conocidas.

- Backdoors/Rootkits. Dejan puertos abiertos que admiten diálogos con apps externas.
- Auto-rooters. Herramienta que automatiza un ataque realizando una secuencia de actividades con el objetivo de penetrar un sistema.
- Password-crackers. Utilidad que permite averiguar contraseñas de los usuarios mediante técnicas de diccionario, fuerza bruta o ingeniería social.
- Generadores de malware.

Defensa en profundidad

Estrategia que consiste en introducir múltiples capas de seguridad que permitan reducir la probabilidad de compromiso en caso de que una de las capas falle y en el peor de los casos minimizar el impacto.

Medidas de defensa

➔ ***Defensa en políticas, procedimientos y concienciación***

Se definen objetivos, actividades de control y el criterio en la realización de auditorías.

➔ ***Defensa en cortafuegos (firewall)***

Es la primera línea de defensa de la red. Analiza las conexiones entre las redes interna y externa de una organización y restringe el acceso de acuerdo con una política de seguridad.

➔ ***Defensa en el sistema de detección de intrusos (IDS)***

Monitoriza el tráfico de red y alerta/previene de cualquier actividad potencialmente sospechosa en tiempo real.

➔ ***Defensa en el control de acceso a la red (NAC)***

Permite inspeccionar los sistemas que se conectan a la red para dilucidar si cumplen o no las políticas de seguridad requeridas por el administrador de la red.

➔ ***Defensa contra malware***

Protege al sistema de amenazas como virus, troyanos, etc.

➔ ***Defensa mediante cifrado***

Protege de muchos ataques, especialmente de confidencialidad, integridad y autenticidad.

➔ ***Defensa de equipamientos físicos***

Auditoría de seguridad

Consisten en la realización de una valoración de la seguridad de los sistemas informáticos. Se analizan las vulnerabilidades y riesgos al que exponen los sistemas y la posible capacidad de ataque.

La **gestión del riesgo** ("*RISK MANAGEMENT*") se compone de cuatro fases:

- ❖ Análisis, determinar componentes vulnerables, sus vulnerabilidades y las amenazas a los que se expone.
- ❖ Clasificación, riesgos son asumibles o hay que actuar contra ellos.
- ❖ Reducción, define e implementa medidas de protección.
- ❖ Control, analiza el funcionamiento, la efectividad y el cumplimiento de medidas para ajustarlas.

Hacer una auditoría al año.

Tipos de auditoría

Se clasifican en:

- ***Auditoría de la red interna***, examina la LAN de la organización, así como los sistemas que se conecten a ella.
- ***Auditoría de la red perimetral***, encargada de analizar redes y servicios que se publican en internet.
- ***Auditoría de test de intrusión***, evalúa el riesgo comprobando la resistencia del sistema a posibles ataques.
- ***Auditoria forense***, posterior al ataque con objetivo de averiguar cómo se produjo para evitarlo.

Control de acceso

Primera barrera que el atacante debe superar:

- Equipos de escritorio: deberán proteger con seguridad externa al propio equipo.
- Servidores: acceso físico restringido a la sala de servidores mediante llaves, tarjetas de acceso o controles biométricos.

Recomendación en contraseñas

- Longitud mínima, números, símbolos, mayus y minus.
- Cadenas que no estén en diccionarios.
- Caducidad de contraseñas
- No coincidente a la anterior
- Combinar tarjetas de seguridad.

Seguridad de la BIOS

- La BIOS necesita contraseña, protegiendo así la elección del disco de arranque.
- Los ataques o manipulación de la BIOS puede ocasionar muchos problemas:
    - Ataques de denegación de servicios. Equipo no arranca el disco adecuado e impide acceso al sistema.
    - Ataques de suplantación. Arrancar un disco alternativo, simulando el original.
    - Pérdidas de información. Copia de datos a un liveCD o formateo de particiones.
- Se deberá tener acceso para cambiar su config. No arrancar mediante CD o Pendrive.

Actualización de sistemas y aplicaciones

La actualización de sistemas reduce las vulnerabilidades disminuyendo la superficie de ataque. Hacer copias de seguridad previa a las actualizaciones.
Otras razones para realizarlas:

- Nuevas mejoras
- Nuevas funcionalidades
- Compatibilidad con nuevas plataformas.
- Compatibilidad con nuevos componentes hardware.

Cuando actualizar

Cuanto antes mejor.
Modo: manual o automático.

Seguridad en Discos y Ficheros

Si un atacante penetra en el sistema se encontrará con otra barrera cuando quiera acceder al sistema de ficheros.

Seguridad en el particionado de discos

- Escoger cuidadosamente cómo establecer el particionado de discos, especialmente en servidores.
- Errores en el particionado provocan denegación de servicio acceso libre al malware.
- Un mal diseño de capacidad, hará que colapsen los discos y no den servicio continuado.
- En linux tener cuidado con las particiones /var y /home, se rellenan con facilidad. Se separa normalmente “/” de “/home”.

Seguridad en los sistemas de ficheros

Sistemas expuestos a corrupción de datos y deterioro de los sistemas. Frecuentemente los procesos de escritura se quedan a medias y no se guardan, corrompiendo los archivos.

Usar sistemas de ficheros transaccionales como ext4 para Linux o NTFS para Windows, que garantizan la atomicidad de las operaciones.

Listas de accesos controlados

ACL: conjunto informático que describe un conjunto de entidades sobre el que se definirán una regla de acceso controlado.
Una vez definido el conjunto se le asigna la aceptación o denegación de una operación o acceso. Conjunto de listas conocido como políticas de acceso.
En linux se usa:

- ***chown***: cambia propietario
- ***chgrp***: cambia grupo
- ***chmod***: cambia permisos

Autenticación de acceso al sistema

Distintas personas = distintos usuarios.
A estas cuentas se le asignan estos permisos y derechos que se ciñan a su posición dentro del sistema. Se debe considerar:

- Deshabilitar cuentas conocidas. tener las conocidas.
- Restricciones en el log-on de usuarios. asignar horarios de uso.
- Política de contraseñas, cambio de contraseña iniciales.
- Otros medios de control:tarjetas de banda magnética, chips, etc.

Ataques de malware

Malware: cualquier tipo de procedimiento, programa que está diseñado con el objetivo de atacar un sistema o proceso.

- ➔ Virus: secuencia de instrucciones con capacidad de autorréplica.
- ➔ Ransomware: secuestro de archivos.
- ➔ Gusanos: programas independientes con capacidad de autoreplica.
- ➔ Troyano: de apariencia inofensiva.
- ➔ Backdoors o Rootkit: establecer puertas traseras de acceso al sistema.
- ➔ Spyware: recopilar información valiosa del sistema.
- ➔ Keylogger: recoge pulsaciones del teclado.
- ➔ Adware: integra publicidad no deseada.
- ➔ Spam: recepción de correo no deseado.

Malware tiene como objetivo burlar la seguridad de un sistema o explotar vulnerabilidades.

Seguridad en la conexión de redes públicas

Una conexión a una red supone un aumento de la exposición a los ataques.
Los riesgos son:

- Cortafuegos no configurado correctamente.
- Transmisión de información en texto plano.
- Conexiones telnet y ftp no cifradas.
- Servidores de red expuestos y filtrado de información.
- Sesiones abiertas en servidores.
- Denegación de servicio.

Medidas contra los riesgos de red

Se pueden reducir los riesgos integrándose en el plan de seguridad:

- ❖ Disponer de un antivirus de calidad y actualizado.
- ❖ Tener activado y bien configurado el firewall.
- ❖ Integrar el antivirus en una suite de seguridad que provea otros servicios de seguridad.
- ❖ Proteger las conexiones mediante cifrado
- ❖ Utilizar VPN
- ❖ Validar conexiones remotas.

Estrategias de defensa

Se debe estar informado de las técnicas de hacking actualizadas y de qué amenazas nos tendremos que defender.

Medidas generales

- ★ Deshabilitar servicios no utilizados. Desinstalar mejor.
- ★ Utilizar combinación firewall y proxy.
- ★ Informarse de las últimas vulnerabilidades encontradas sobre el software instalado.
- ★ Aplicar parches y actualizaciones tan pronto como sea.

Contramedidas específicas

Para linux:

- Seguir sugerencias de los portales de seguridad
- Utilizar Nessus o COPS para evaluar niveles de seguridad.
- Al ser de código libre, habrá información de programas y apps que queramos estudiar en profundidad.

Para windows:

- Bloquear el acceso de los puertos 135-139 tanto en TCP como UDP.
- Deshabilitando la cuenta de invitado.
- Habilitar la encriptación de la administración de cuentas de seguridad con SYSKEY.

Seguridad en redes corporativas

Niveles de seguridad:

- ➔ Niveles 1 y 2: capa de red TCP/IP. Acceso físico a comunicaciones.
- ➔ Nivel 3: capa de internet TCP/IP. Escuchas no autorizadas de paquetes de IP, suplantación de IP.
- ➔ Nivel 4: capa de transporte. La falta de protección de puertos por el firewall puede provocar DoS.
- ➔ Nivel 5 al 7: se prestan a problemas asociados a los servicios de red y a la autenticación de datos.

Ataques de una red TCP/IP

Persuasión velada a los usuarios para que ejecuten acciones o revelen información que el atacante necesita para comprometer la red. Se deduce la info del target que será atacado: fechas, aniversarios, etc. Obtenemos informes sobre ciertos aspectos de la seguridad de la web con herramientas como Web Spider.

Ataque de DoS

Impide el uso legítimo del sistema atacado por parte de los usuarios autorizados.
Provocado por consumo excesivo de recursos del servidor.
El ataque se esconde detrás de una red de atacantes compuesta de sistemas infectados. Su defensa se realiza bloqueando la dirección IP del atacante para que no consuma recursos.

Tipos de DDoS

- ➔ ***Net Flood***

Degrada la conectividad de una red mediante la saturación de sus enlaces de comunicación. Organiza ataques masivos desde diferentes puntos de la red mediante zombies o botnets. La defensa hoy en día es escasa.

- ➔ ***Connection Flood***

Todo servicio orientado a la conexión tiene un límite máximo en el número de conexiones simultáneas que soporta.

- ➔ ***SYN Flood***

Se basa de nuevo en las conexiones TCP/IP. Si el paso final no se realiza, la conexión queda semiabierta.

Cracking de contraseñas, mail bombing y spaming

- ***Cracking de contraseñas***: proceso de robo de credenciales. Principalmente usuarios con permisos y privilegios. Estos ataques pueden ser:
    - De fuerza bruta: realiza todas las combinaciones posibles de un conjunto de caracteres y una longitud máxima.
    - De diccionario: efectúa un ataque ordenado utilizando combinaciones típicas registradas en un archivo.
- ***Mail bombing***: envía un mensaje a un usuario en múltiples ocasiones para provocar una DoS. Perjudicado: cliente.
- ***Spaming***: orientado a enviar mensajes no deseados a múltiples buzones. Genera problemas en los buzones de destino y en el servidor emisor.

Escaneo de puertos

Ataques centrados en los puertos abiertos.
Se buscan vulnerabilidades en los servicios que se encuentran en dichos puertos.
Tienen importancia las actualizaciones del sistema y aplicaciones.
Algunos cortafuegos podrán detectar actividades de rastreo de puertos.

Sniffers

Operan activando la interfaz de red del sistema el que se ejecuta en modo promiscuo.
Almacenan en un log el tráfico de red en el punto por el que se conecta la escucha.
El uso de sniffers permite obtener información sensible sin descifrar: nombres de usuario, contraseña, correo, etc.
Condición: la info tiene que pasar por el puerto en el que está conectado.
En redes conmutadas no ocurre ya que solo pasan por el puerto el tráfico con origen y destino en el sistema.

Desbordamientos de buffer

Aprovecha errores de programación de una aplicación para alterar el funcionamiento de la pila de un proceso. Son producidos por:

➔ **Overflow por combinaciones no esperadas**

Los programas suelen instalarse formando capas de códigos instaladas jerárquicamente en el SO. Un mal diseño causaría entradas de capas superiores enviadas directamente al SO.

➔ **Overflow por entrada anormal**

Los programas tienen un rango de parámetros válidos. Si el código no valida correctamente la entrada del usuario, puede provocar daños en los datos que maneja la aplicación.

➔ **Overflow por ocurrencia**

2 o más procesos leen o escriben sobre un área compartida por ambos. Si no hay control sobre el proceso, el resultado depende de la secuencia temporal.

Ataques internos en LAN conmutadas

Principales ataques:

➔ ***Inundación de direcciones MAC***

Produce una sobrecarga de la tabla CAM del conmutador para producir su desbordamiento.

➔ ***IRDP spoofing***

Protocolo que amplía ICMP para que pueda descubrir enrutadores en el entorno de red. El hacker se hace pasar por router.

➔ ***ARP poisoning***

Produce envenenamiento de la tabla ARP utilizada por los equipos para la resolución IP en direcciones MAC. Etthercap, Nemesis o Caín

Riesgos potenciales en los servicios de red

Los clientes consumen recursos de la red en forma de servicios.
Minimizar la superficie de exposición. Solo instalar servicios que se utilicen. Ejemplo:

- Firewall, abierto los puertos de los servicios que se usen.
- Instalar y activar los servicios necesarios.
- Elegir procesos que estén cifrados y cuenten con autenticado.

Los puertos de servicios de red.

En IPv4 los puertos se expresan con 16 bits por lo que se generan 2^16 puertos.
Se clasifican en:

- Puerto 0: reservado, no se usa.
- Puertos 1 - 1023, puertos bien conocidos.
- Puertos 1024 - 49.151, puertos registrados. Libres.
- Puertos 49.152 - 65.535, efímeros o temporales.

Abrir un puerto significa autorizar al cortafuegos para permitir comunicaciones por ese puerto.