SEGURIDAD Y ALTA DISPONIBILIDAD

2º DE ADMINISTRACIÓN DE SISTEMAS INFORMÁTICOS EN RED

Noelia Huguet Chacón

TOBALCAIDE

TEMA 5: GESTIÓN ACTIVA DE LA SEGURIDAD

1. La seguridad activa en los sistemas
2. La defensa en profundidad en sistemas personales
3. Seguridad en la red corporativa
4. Seguridad y monitorización

3.1 LA SEGURIDAD ACTIVA EN LOS SISTEMAS

- Una vez que ha sufrido un ataque, lo mejor que le puede suceder a un administrador de seguridad es conocer el objetivo del atacante y el método de ataque que ha perpetrado.
- Está información le proporcionará pistas clarificadoras sobre el camino que debe tomar para organizar la defensa.
- Por tanto, es importante conocer las características que definen tanto al atacante como al ataque.
- En el argot de la seguridad los atacantes suelen clasificarse por:
  - Su actividad
  - Su relación con el objeto del ataque.

3.1.1 EL PERFIL DEL ATACANTE Y SU MOTIVACIÓN

CLASIFICACIÓN DE ATACANTES POR SU ACTIVIDAD:

- **HACKER**: Es una persona con amplios conocimientos tecnológicos que mantiene actualizados permanentemente. Tiene una gran deseo por conocer exhaustivamente los sistemas de cifrado y las posibilidades de acceso a cualquier sistema inseguro sin ser descubierto. Ocasionalmente, el hacker puede ser contratado por las empresas para aprovechar sus profundos conocimientos sobre seguridad: se habla de que se ha convertido en un **hacker de sombrero blanco**.
- **CRACKER:** Es un atacante de comportamiento compulsivo obsesionado con asaltar sistemas informáticos y electrónicos o saltarse las claves de protección de aplicaciones de software. El cracker es un gran conocedor de la programación y llega a diseñar software para reventar todo tipo de sistemas.
- **BUCANERO:** Es el comerciante ilegal de la red. No posee formación técnica significativa pero sí en el área de negocios, lo que frecuentemente aprovecha para cometer fraudes.

3.1.1 EL PERFIL DEL ATACANTE Y SU MOTIVACIÓN

CLASIFICACIÓN DE ATACANTES POR SU ACTIVIDAD:

- **LAMMER**: Es una persona que desea convertirse en un hacker pero a la que su escaso nivel formativo le supone una gran barrera para conseguirlo. Se dedica a ejecutar programas creados por otros o a descargar indiscriminadamente cualquier aplicación publicada en la web. Frecuentemente, la amenaza del lammer reside en que no controla los efectos del ataque que perpetra. En los primeros estadios de conocimiento, los lammers reciben la denominación de **newbies**.
- **COPYHACKER:** Es un falsificador de hardware, fundamentalmente de tarjetas inteligentes. Se relacionan con hackers, copian sus métodos de ruptura de sistemas y después los venden, por lo que su principal motivación no es técnica sino económica.
- **PHREAKER:** Posee robustos conocimientos sobre telefonía que aprovecha en su propio beneficio para actividades ilegales.
- **KIDDIE:** Son simples usuarios de Internet que ponen en ejecución cualquier cosas que puedan descargar sin ningún conocimiento de lo que hace e infectando de virus y malware sus propios equipos, poniendo en riesgo los de otros.

3.1.1 EL PERFIL DEL ATACANTE Y SU MOTIVACIÓN

CLAS. DE ATACANTES POR SU RELACIÓN CON EL OBJETO DEL ATAQUE:

- **SNIFFERS**: Son individuos que se dedican a escuchar ilegalmente la red para reconstruir y descifrar los mensajes que circulan en ella.
- **SPAMMERS:** Gestionan el envío masivo e indiscriminado de millones de mensajes de correo electrónico no solicitado, lo que provoca el colapso tanto de los servidores como de los buzones de los destinatarios.
- **PROGRAMADORES DE MALWARE**: son expertos programadores que construyen virus y otros programas maliciosos que buscan notoriedad intentando lograr una propagación desbordante.
- **PERSONAL INTERNO A LA ORGANIZACIÓN**: Son usuarios incorporados a la organización que por despiste, curiosidad, malicia o ingenuidad pueden causar daño a la organización.
- **ANTIGUOS EMPLEADOS:** Son personas que pertenecieron a la organización y que por despecho o venganza actúan contra su antigua empresa aprovechando sus cuentas de usuario aún no canceladas.
- **INTRUSOS REMUNERADOS:** son personas expertas en informática contratadas por un tercero para perpetrar ataques relacionados con la fuga de información confidencial o para provocar sabotajes en los sistemas de la organización que atacan.

3.1.1 EL PERFIL DEL ATACANTE Y SU MOTIVACIÓN

LA MOTIVACIÓN DEL ATACANTE:

- ¿Qué hace un atacante perpetre un ataque?
  - Las motivaciones son muy variadas y frecuentemente no se dan aisladas.
  - Entre las motivaciones más usuales se encuentran:
    - El dinero u otras motivaciones de naturaleza económica.
    - La ideología, por ejemplo, en el caso de ataques terroristas o la pertenencia a grupos.
    - El compromiso con ciertas personas u organizaciones, a veces bajo presión.
    - La autorrealización personal, el reconocimiento social o la mejora del status social, que se da sobre todo en personas con deficiencias relacionales.
    - La diversión.

3.1.1 EL PERFIL DEL ATACANTE Y SU MOTIVACIÓN

RIESGOS ASOCIADOS CON LAS PERSONAS

- La ignorancia es el mayor riesgo que concurre en una persona, pero se combate con una contramedida tan sencilla como la formación de los usuarios del sistema.
- Sin embargo, no pueden despreciarse otros peligros que exigen tomar contramedidas alternativas que atenúen la valoración del riesgo que comportan.
  1. Intrusos o atacantes que utilizan ingeniería social para averiguar o intuir las claves de acceso de las cuentas de usuario legales.
  2. Configuración incorrecta de cuentas de usuario, grupos, permisos, derechos… Reticencia a cancelar cuentas, ficheros, derechos de usuarios que ya no existen o no los necesitan.
  3. Incumplimiento de las directivas o políticas de seguridad.
  4. Errores en la documentación de los sistemas, de sus configuraciones o en la comunicación de esa documentación a técnicos o usuarios. También pueden aparecer problemas cuando se descuida la custodia de esta documentación.

3.1.1 EL PERFIL DEL ATACANTE Y SU MOTIVACIÓN

- **RIESGOS ASOCIADOS CON LAS PERSONAS**

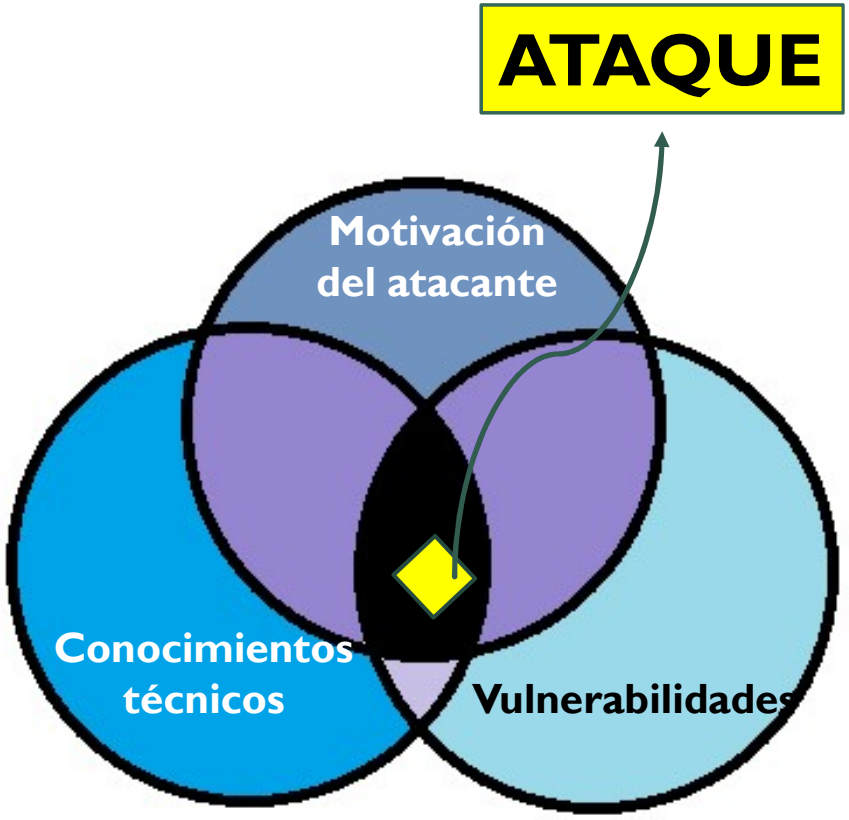
5. Empleados descontentos o deshonestos que abusan de sus derechos de acceso a la información.
6. Equipos erráticos que nadie controla, que conservan derechos o funciones heredados.
7. Utilización de contraseñas inseguras, especialmente por administradores o usuarios con acceso a informaciones especialmente sensibles.
8. Usuarios que habilitan puertas traseras en sus equipos a través de las que se pueden ejecutar ataques desde el exterior.
9. Déficit en el tratamiento de medios de almacenamiento desechables.
10. Contraseñas escritas en papel.

3.1.2 EL ATAQUE INFORMÁTICO

- El ataque de un sistema, una vez decidido su objetivo, acostumbra seguir un conjunto ordenado de pasos para llevar a cabo su ataque.
- Previamente ha tenido que decidir qué sistema de todos los que están a su alcance es el más apropiado para su actividad.
- A grandes rasgos, **las fases de un ataque** se resumen en las siguientes actividades:
  1. Descubrimiento de los sistemas que componen la red en la que se halla el objeto.
  2. Exploración de las vulnerabilidades de los sistemas de la red.
  3. Explotación de las vulnerabilidades detectadas.
  4. Compromiso del sistema.
  5. Ocultamiento o eliminación de los rastros que prueban el ataque.

3.1.2 EL ATAQUE INFORMÁTICO

- Las vulnerabilidades se explotan mediante herramientas específicamente construidas para tal fin que se denominan "**exploits**".
- La corrupción del sistema consiste en la modificación del software o los datos residentes en el sistema para inocular puertas traseras o troyanos, creación de cuentas errantes con privilegios… que pueden ser explotadas remotamente por el atacante.
- La eliminación de las pruebas del ataque consistirá en borrar los ficheros de log de actividad del sistemas o alteración del comportamiento de los procesos que revelan la actividad del sistema como en el caso de los rootkits.



3.1.2 EL ATAQUE INFORMÁTICO

TIPOS DE ATAQUES INFORMÁTICOS COMUNES

- Los principales ataques a un Sistema Informático se organizan en torno a las siguientes actividades:
  - Acciones de reconocimiento y descubrimiento de dispositivos y sistemas.
  - Detección de vulnerabilidades.
  - Robo de información mediante la interceptación de tráfico.
  - Cifrado de información almacenada con claves solo conocidas por el atacante, que cederá a la víctima bajo rescate económico (**ransomware**)
  - Modificación de contenidos en los mensajes intercambiados por la red.
  - Alteración de los números de secuencia en los mensajes transmitidos.
  - Análisis de tráfico de red.
  - Suplantación de la identidad de los agentes de procesos.

3.1.2 EL ATAQUE INFORMÁTICO

TIPOS DE ATAQUES INFORMÁTICOS COMUNES

- Los principales ataques a un Sistema Informático se organizan en torno a las siguientes actividades:
  - Alteración de las tablas de enrutamiento, tablas de direcciones físicas…
  - Conexión no autorizada a los sistemas de la red, lo que da paso a la introducción de malware, fraudes, extorsiones, ataques criptográficos…
  - Denegaciones de servicio, tanto simples (DoS, Denial of Service) como distribuidos (DDoS, Distributed Denial of Service)
  - Propagación de malware.
  - Alteración o destrucción de información.

3.1.2 EL ATAQUE INFORMÁTICO

HERRAMIENTAS UTILIZADAS EN UN ATAQUE

- Para ejecutar el ataque, el atacante utiliza herramientas apropiadas para el tipo de ataque que desea perpetrar y de lo objetivos que pretende conseguir con él.
- Estas herramientas tiene un alto grado de sofisticación y ataque se adecuan al ataque concreto.
- También hay que considerar que un ataque suele requerir varias de estas herramientas, ejecutadas en una secuencia determinada, para conseguir objetivos intermedios desde los que escalar mayores privilegios, crackear contraseñas, introducir malware…
- Además de las siguiente utilidades específicas, los atacantes suelen tener elevados conocimientos sobre técnicas de ocultación y suplantación, así como de criptografía.
- Las herramientas más comunes:
  - **Escáneres de puertos:** permiten detectar los servicios instalados en el sistema en que se ejecutan (escáner local) o en otro sistema remoto (escáner de puertos remotos).
  - **Sniffers o escuchadores de red**: son dispositivos o aplicaciones que escuchan la red para capturar los paquetes de datos que circulan en ella.

3.1.2 EL ATAQUE INFORMÁTICO

HERRAMIENTAS UTILIZADAS EN UN ATAQUE

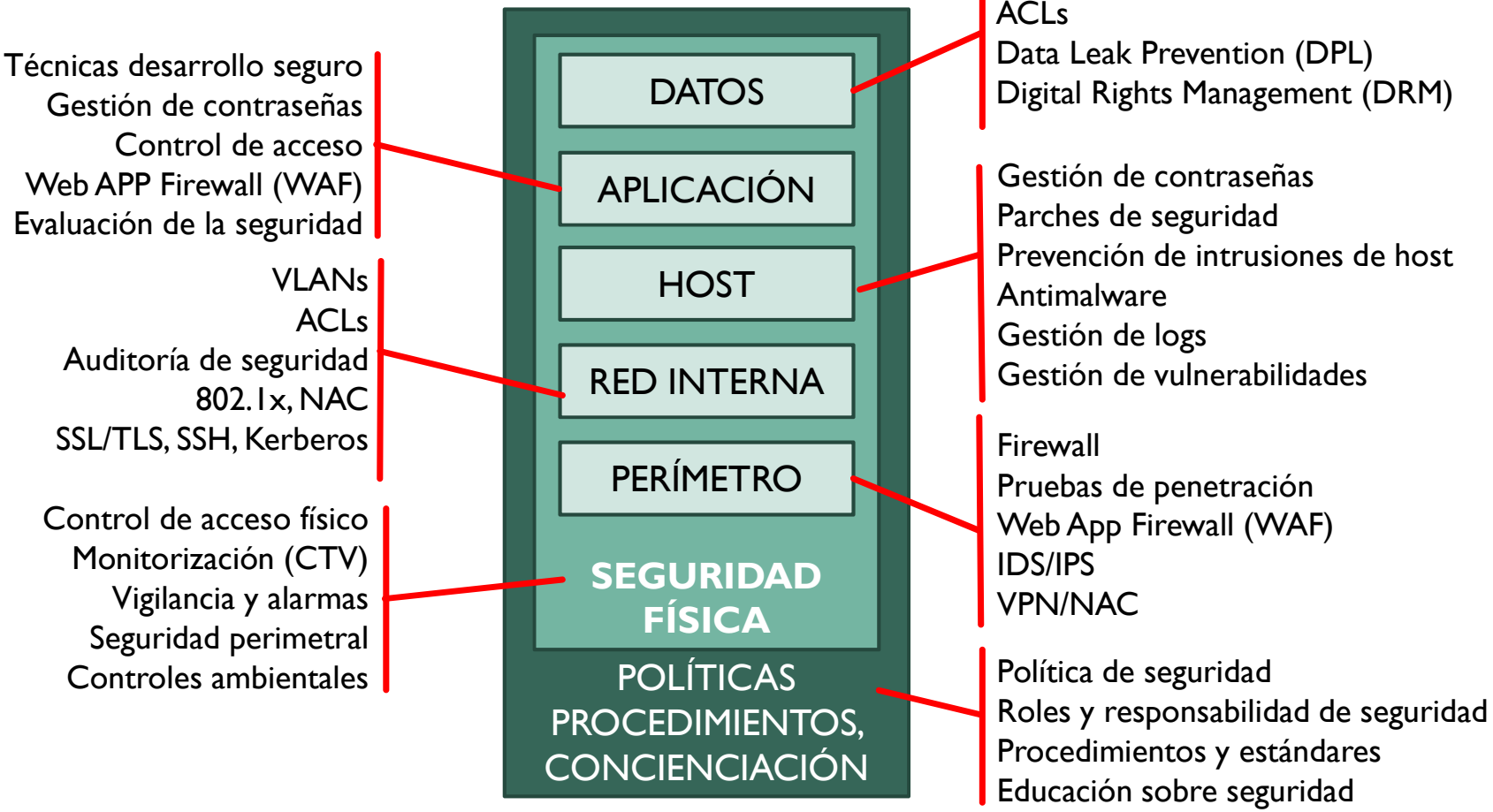
- Las herramientas más comunes:
  - **Exploits**: son herramientas que buscan y explotan vulnerabilidades conocidas de los sistemas sobre los que se ejecuta el ataque o bien sistemas desde los que se pretende llevar a cabo el ataque.
  - **Backdoors o puertas traseras**: son aplicaciones que permiten abrir agujeros de seguridad en los sistemas, habitualmente dejando puertos abiertos que admiten diálogos con aplicaciones externas dirigidas por el atacante.
  - **Rootkits:** son utilizados por los atacantes para ocultar malware, frecuentemente puertas traseras, por lo que despistan al sistema de vigilancia del propio sistema o de las suites de seguridad.
  - **Auto-rooters**: son herramientas capaces de automatizar un ataque realizando la secuencia de actividades encaminada a obtener el acceso al sistema o explotar una vulnerabilidad.
  - **Password-crackers:** son utilidades que permiten averiguar las contraseñas de los usuarios mediante técnicas de diccionario, fuerza bruta o ingeniería social.
  - **Generadores de malware**: son aplicaciones especialmente diseñadas para la generación de virus u otro tipo de malware.

3.2.1 LA DEFENSA EN PROFUNDIDAD

- La seguridad física consiste en la aplicación de contramedidas tales como barreras físicas o procedimientos de control que prevengan amenazas contra los recursos que se pretenden proteger, disminuyendo los riesgos.
- La seguridad de los sistemas debe organizarse según las propuestas de una defensa en profundidad, es decir, debe proveer múltiples barreras con seguridad integrada en cada una de ellas.
- La definición formal que proporciona el Centro Cristológico Nacional Español es:
  - **La defensa en profundidad es una estrategia consistente 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.**
- Esta organización en niveles permite dividir el problema global de la seguridad en otros más pequeños y manejables con soluciones altamente especializadas, contribuyendo de este modo a mejorar la calidad de la implantación del plan de seguridad.
- En función del momento en que se activa la contramedida o medida de seguridad esta puede ser reactiva (tipo pasivo) o proactiva (activa o preventiva), según si se activa como reacción a un incidente o bien antes de que se produzca como medio de prevención.
- Sin embargo, si atendemos al tipo de recurso protegido, las contramedidas pueden ser físicas o lógicas.

3.2.1 LA DEFENSA EN PROFUNDIDAD

- **Niveles de una defensa en profundidad.**



3.2.1 LA DEFENSA EN PROFUNDIDAD

MEDIDAS DE DEFENSA

- **Defensa en políticas, procedimientos y concienciación.** Establecen el tono de seguridad en toda la organización en relación a la protección de activos informáticos, defines los objetivos y actividades de control y proveen un criterio para **la realización de auditorías.** Para mejorar su efectividad, las políticas deben ser comunicadas a todo el personal de la empresa ya que la concienciación es un elemento clave. Debe exigirse a todo el personal un compromiso serio con la seguridad.
- **Defensa en cortafuegos.** La primera línea de defensa de la red es el cortafuegos (**firewall**), que analiza las conexiones entre las redes interna y externa de una organización y restringe el acceso con una política de seguridad. Actualmente al cortafuegos se le han añadido otras funciones de seguridad que antiguamente estaban dispersas, pero sigue siendo el principal activo de seguridad en la red, siempre que sea correctamente gestionado: uno de los mayores peligros en pensar que se tiene el cortafuegos correctamente configurado cuando en realidad no sea así porque no esté actualizado, porque las reglas que componen la política de acceso no estén bien configuradas o porque no se auditen correctamente los eventos.

3.2.1 LA DEFENSA EN PROFUNDIDAD

MEDIDAS DE DEFENSA

- **Defensa en el sistema de detección de intrusos (IDS).** Es un sistema que monitoriza el tráfico de la red y alerta o previene de cualquier actividad sospecha en tiempo real. Son sistemas que generan una gran cantidad de falsos positivos, es decir, detectan algunas actividades legítimas como si fueran maliciosas, lo que hay que vigilan constantemente para minimizarlos y que ello no interrumpa la actividad de producción de la red. Algunos IDS también pueden implantar procesos específicos de intervención para atajar los problemas de seguridad detectados.
- **Defensa en el control de acceso a la red (NAC).** Un buen control de acceso 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. Por ejemplo, podría determinarse que cualquier ordenador que se conecte a una red debe tener su antivirus actualizado y su cortafuegos personal activado. Si el sistema no cumpliera con los requisitos exigidos, se le puede denegar el acceso o permitirle una conexión solo a ciertos segmentos de la red.

3.2.1 LA DEFENSA EN PROFUNDIDAD

MEDIDAS DE DEFENSA

- **Defensa contra malware.** Las tecnologías antimalware, que protegen de amenazas como virus, troyanos, botnets, spyware y otras formas de código malicioso, continúan avanzando para presentarse a los usuarios como auténticas suites de seguridad altamente sofisticadas. Sin embargo, para que sean eficaces deben ser correctamente gestionadas.
- **Defensa mediante cifrado.** El cifrado de datos protege de muchos ataques, especialmente los de confidencialidad, integridad y autenticidad. De este modo, aunque el resto de controles hayan sido violados aún quedará una barrera importante. Debemos recordar que la seguridad del cifrado depende de la custodia de una clave o contraseña por lo que habrá que protegerla con sumo cuidado.
- **Defensa de los equipamientos físicos.** Aunque se tenga un buen sistema de defensa lógica, de nada servirá si no se cuida la seguridad física. Por tanto, es imprescindible mantener controles de seguridad física como cámaras, alarmas, vigilancia… Siempre es importante, pero cobra especial relieve en lugares como el centro de proceso de datos.

3.2.1 LA DEFENSA EN PROFUNDIDAD

EL CONTROL DE ACCESO AL SISTEMA

- La primera medida de protección de un sistema consiste en impedir el acceso físico al mismo.
- En los equipos de escritorio, esto es imposible puesto que los usuarios trabajan delante de los equipos físicos, por lo que en estos casos hay que habilitar medidas alternativas equivalentes.
- En los servidores, la protección se hace más fácil (basta con que estén bajo llave o en un lugar reservado), pero también más necesaria por el grado de compromiso que se pone en entredicho en caso de ataque.
- En este caso, el acceso a las salas de servidores debe estar monitorizado y controlado mediante tarjetas de acceso o sistemas biométricos.

3.2.1 LA DEFENSA EN PROFUNDIDAD

EL CONTROL DE ACCESO AL SISTEMA

- Para diseñar un buen sistema de acceso seguro a las instalaciones se puede reflexionar sobre las siguientes cuestiones o tecnologías:
  - ¿Qué salas contiene sistemas críticos y deben ser protegidas?
  - ¿Qué formas de acceso podrían utilizar los intrusos?
  - Definición de los horarios de acceso permitidos para cada usuario.
  - Instrucción de los empleados sobre el sistema de acceso.
  - Métodos de autenticación permitidos en la organización.
  - Chequeos periódicos del sistema de seguridad (auditoría).
  - Cambio frecuente de contraseñas como parte de la política de seguridad.
  - Creación de un plan de seguridad y de respuesta frente a brechas.
- A partir de aquí debe diseñarse la seguridad lógica. La parte más importante de esta seguridad es una buena política de gestión de contraseñas, una buena política de contraseñas incrementa notablemente la seguridad de los sistemas.

3.2.1 LA DEFENSA EN PROFUNDIDAD

EL CONTROL DE ACCESO AL SISTEMA

- Para crear una buena política de contraseñas se podría considerar algunos o todos los factores siguientes en función de las exigencias de seguridad:
  - Longitud mínima de las contraseñas de las cuentas de usuario.
  - Caducidad de las contraseñas.
  - No permitir que la renovación de una contraseña coincida con una anterior del mismo usuario.
  - Exigir contraseñas complejas, que contengan caracteres alfabéticos en mayúsculas y minúsculas, símbolos y números.
  - Combinar el uso de contraseñas(algo que el usuario sabe) con tarjetas de seguridad (algo que el usuario tiene).
  - Auditar todos los accesos de usuario en el sistema, así como los cambios de contraseñas o las alteraciones de privilegios de las cuentas.

3.2.1 LA DEFENSA EN PROFUNDIDAD

LA SEGURIDAD EN LA BIOS Y EN LOS GESTORES DE ARRANQUE

- Algunas de las características básicas de los equipos se configuran en las BIOS del sistema, cuyo acceso siempre debe estar protegido con una contraseña.
- Esta contraseña suele ser muy débil pero ya es una primera barrera.
- Algunas BIOS también pueden proteger mediante contraseña la posibilidad de arrancar de un disco o de otro, de modo que solo quien conozca esta contraseña podrá arrancar el sistema.
- La alteración o manipulación de la BIOS puede originar muchos problemas:
  - **Ataques de denegación de servicio.** Por ejemplo, el equipo no arranca del disco adecuado y se impide el acceso al sistema contenido en él. También, desde la BIOS, se puede deshabilitar parte del hardware.
  - **Ataques de suplantación.** Por ejemplo, se puede arrancar de un disco alternativo, que simula ser el original, pero que contiene software que compromete la privacidad del usuario que cree presentarse en un sistema habitual.
  - **Pérdidas o fugas de información.** Como ejemplo, se puede arrancar de un LiveCd y se copian los datos del sistema objetivo o se formatean sus particiones. También se podrían suplantar las contraseñas de cuentas privilegiadas.

3.2.1 LA DEFENSA EN PROFUNDIDAD

ACTUALIZACIÓN DE SISTEMAS Y APLICACIONES

- La actualización de los sistemas y aplicaciones es una de las actividades más importantes que se pueden realizar para mejorar sustancialmente la seguridad de un sistema porque reduce sensiblemente el número de vulnerabilidades disminuyendo la superficie de ataque.
- Aun así, una actualización comporta algún riesgo: no debe realizarse nunca una actualización sin practicar una copia de seguridad probada, si algo saliera mal durante la actualización o el comportamiento del sistema después de la actualización fuera errático, se podría volver atrás restaurando el backup realizado.
- Pero, esta no es la única razón que aconseja actualizar el sistema y sus aplicaciones, aunque sí es la más relacionada con la seguridad.
- Otras razones son las siguientes:
  - Eliminar vulnerabilidades detectadas por el desarrollador de la aplicación o del sistema operativo (bugs)
  - Incorporación de mejoras en el software, por ejemplo, incrementando el rendimiento o la usabilidad.
  - Adición de nuevas funcionalidades que mejoran la aplicación.
  - Compatibilidad con nuevas plataformas tecnológicas de software de sistemas.
  - Compatibilidad con novedades en el hardware.

3.2.1 LA DEFENSA EN PROFUNDIDAD

ACTUALIZACIÓN DE SISTEMAS Y APLICACIONES

- Por otra parte, no solo se puede actualizar el software de aplicación o de sistemas.
- Otros elementos actualizables son el firmware de los distintos componentes de hardware, la BIOS, los controladores de dispositivos…
- Los desarrolladores suelen proveer parches o actualizaciones periódicamente para que los usuarios los descarguen y apliquen en sus sistemas, pero como operación no está exenta de riesgo.
- Algunas actualizaciones, que son de bajo o nulo riesgo, pueden ser realizadas directamente por los usuarios de las aplicaciones, sin embargo, los sistemas suelen defenderse impidiendo que los usuarios no administradores puedan realizar instalaciones.
- La cuenta de usuario más indicada para cualquier actualización es la de administrador o superusuario.
- Cuando se realizan operaciones delicadas como es una actualización, que puede colisionar con la operación del antivirus, es conveniente desactivar el antivirus del sistemas para que no interfiera (mediante un falso positivo) con la instalación y esta se quede a medio realizar, lo que podría dejar al sistema en un estado inestable.

3.2.2 SEGURIDAD EN DISCOS Y FICHEROS

- Otro nivel de seguridad en la defensa en profundidad se aplica a discos y ficheros.
- Si un atacante es capaz de acceder a un sistema, por ejemplo, por una puerta trasera (backdoor), se encontrará con otra barrera de protección cuando quiera acceder a los sistemas de ficheros.

3.2.2 SEGURIDAD EN DISCOS Y FICHEROS

SEGURIDAD EN EL PARTICIONADO DE DISCOS

- Siempre deben elegirse cuidadosamente las configuraciones en que se van a particionar los discos, especialmente en servidores.
- Cada partición de disco debe llevar asociado una seguridad específica.
- Errores en el diseño de las particiones de los discos originan ataques de denegación de servicios y vía de acceso libre al malware.
- Por ejemplo, si no dotamos a las particiones de disco del suficiente espacio, estas se pueden llenar y ocasionar discontinuidades en el servicio, lo que es un ataque de denegación de servicio en toda regla.
- Otro ejemplo: en una partición de disco formateada como FAT, cualquier usuario (puesto que FAT no admite seguridad de ficheros) puede ejecutar cualquier herramienta al uso y deteriorar el sistema.

3.2.2 SEGURIDAD EN DISCOS Y FICHEROS

SEGURIDAD EN LOS SISTEMAS DE FICHEROS

- Los ficheros que residen en el sistema de ficheros no están exentos de amenazas.
- Las más frecuentes apuntan a la corrupción o deterioro de los sistemas de ficheros en que residen.
- En este sentido, son más seguros los sistemas de ficheros transaccionales con journaling como son ext4 para GNU/Linux o NTFS para Windows, en los que se garantizan que las operaciones de escritura no se quedarán a medias por un fallo de hardware o un corte de suministro eléctrico.
- Otro vector de ataque para los ficheros proviene de los virus u otro tipo de malware.
- Un buen antivirus residente en memoria es una buena defensa, sin embargo, la operación de limpieza no puede nunca garantizar que el fichero desinfectado no quede dañado, bien por la acción malévola del virus o por la ejecución errónea del antivirus en la operación de desinfección.

3.2.2 SEGURIDAD EN DISCOS Y FICHEROS

SEGURIDAD EN LOS SISTEMAS DE FICHEROS

- Por otra parte, un fichero puede ser atacado violando sus permisos de acceso: usuario que no debieran poder acceder al fichero, de hecho, acceden por usurpación de permisos que no les corresponden o por deficiencias en la seguridad del fichero que le ha asignado el administrador.
- Este tipo de ataque se combate mediante una correcta política de accesos controlados.
- Por último, los ficheros deben estar protegidos contra el borrado o manipulación accidental.
- En este caso, un buen sistema de copias de seguridad puede atenuar el riesgo.

3.2.2 SEGURIDAD EN DISCOS Y FICHEROS

LISTA DE CONTROL DE ACCESO, ACL

- Una ACL es un objeto informático que describe el conjunto de entidades (usuarios, equipos, recursos) sobre el que se definirán una regla de acceso controlado.
- Una vez definida la ACL se le asigna un derecho o permiso que básicamente es una denegación o una aceptación de operación o acceso.
- Todas las entidades descritas en la ACL podrán o no acceder al recurso sobre el que se establece la regla.
- Al conjunto de reglas que definen el acceso a un recurso se le denomina política o directiva.
- Un ejemplo de uso común de ACL se encuentra en los routers. Cuando se define una ACL es un router este decide dejar pasar un paquete a su través o eliminarlo de la red en función de si cumple o no unas reglas.

3.2.2 SEGURIDAD EN DISCOS Y FICHEROS

LISTA DE CONTROL DE ACCESO, ACL

- Los recursos compartidos se comportan desde el punto de vista del acceso de los usuarios como si fueran ficheros o carpetas remotos.
- La conexión se realiza o no dependiendo de las reglas establecidas con ACL específicas para recursos de red: carpetas o discos compartidos, impresoras de red…
- Si se desciende al nivel de ficheros, los SO modernos disponen de sistemas de permisos para asignar a cada fichero o carpeta las correspondientes reglas de seguridad.
- Como estos permisos no son compatibles de unos sistemas a otros, por ejemplo, los de Windows con respecto de los de GNU/Linux, esto supone una fuente de vulnerabilidades por deficiencias en la configuración cuando unos sistemas utilizan remotamente los recursos compartidos de otros.

3.2.3 LA AUTENTICACIÓN PARA EL ACCESO AL SISTEMA

- Todo usuario que requiera el consumo de recursos en un sistema seguro debe poseer una cuenta de usuario que lo identifique ante el sistema.
- A esta cuenta se asociarán permisos y derechos que restrinjan las actividades del usuario para que se ciñan a lo que debe ser su función productiva.
- Los administradores deben considerar los siguientes elementos de seguridad relacionados con las cuentas de usuario:
  - Deshabilitar las cuentas conocidas.
  - Creación de una política de restricciones en el logon de los usuarios.
  - Política de contraseñas.
  - Otros medios de control de acceso.

3.2.3 LA AUTENTICACIÓN PARA EL ACCESO AL SISTEMA

DESHABILITAR LAS CUENTAS CONOCIDAS:

- Los sistemas suelen crear por defecto algunas cuentas que deben renombrarse o deshabilitarse para que un intruso no pueda utilizarlas.
- Por ejemplo, en Windows la cuenta Administrador o la cuenta root en GNU/Linux.
- Otras cuentas a tener presente son la de los invitados o guest.

3.2.3 LA AUTENTICACIÓN PARA EL ACCESO AL SISTEMA

Creación de una política de restricciones en el logon de los usuarios

- Por ejemplo, se puede asignar un horario de uso de las cuentas de usuario. Si la jornada laboral es de lunes a viernes, nadie tiene que utilizar esa cuenta un fin de semana, por tanto, esa cuenta no podrá ser atacada cuando no se pueda usar.
- También se puede contabilizar el tiempo total de sesión, de modo que al finalizar el tiempo previsto el sistema despida al usuario automáticamente. Esto impediría, por ejemplo, que si un usuario olvida despedirse quede la sesión abierta indefinidamente.
- Otra restricción común es que ciertos servicios solo pueden ser consumidos desde sesiones establecidas por ciertas direcciones IP y no por otras, o desde la red interna, pero desde Internet.
- Por último, se podría restringir el número de intentos fallidos de presentación de usuario, de manera que, si se sobrepasa un límite, la cuenta utilizada en el intento de intrusión quede bloqueada por un tiempo o permanentemente hasta que un administrador del sistema la desbloquee. De este modo, combatiríamos los ataques de fuerza bruta para crackeo de contraseñas.

3.2.3 LA AUTENTICACIÓN PARA EL ACCESO AL SISTEMA

POLÍTICAS DE CONTRASEÑAS

- Un acceso con contraseña se basa en algo que solo su propietario sabe, que se asocia a un nombre de usuario.
- La política debe tener en cuenta que las contraseñas asociadas a las cuentas de usuario sean suficientemente largas y complejas.
- Además, puede ser convenientemente que se tengan que cambiar frecuentemente, de modo que, si una contraseña es comprometida, lo será solo hasta que su propietario la cambie.
- Recomendaciones para confeccionar contraseñas: cambiar la defecto del sistema, no utilizar información familiar, más de 8 caracteres con símbolos y mayúsculas y minúsculas, no utilizar siempre la misma contraseña, cambiar cada 60 días…

3.2.3 LA AUTENTICACIÓN PARA EL ACCESO AL SISTEMA

OTROS MEDIOS DE CONTROL DE ACCESO

- El uso de tarjetas inteligentes establece la seguridad basada en algo que el usuario "tiene".
- Las hay de diversos tipos: tarjetas con banda magnética como las tarjetas de crédito, tarjetas con chip como el DNIe o sencillamente un pendrive con un contenido específico y protegido.
- Todas estas tarjetas utilizan técnicas criptográficas.
- Otro sistema de control de acceso son los sistemas biométricos, cuya seguridad se base en algo que se "es": una huella dactilar, el iris ocular, un patrón facial…
- En el caso en el que se requieran sistemas de muy alta seguridad se pueden combinar varios de estos sistemas de autenticación.

3.2.4 ATAQUES CON SOFTWARE MALICIOSO

- Se entiende por malware o software malicioso todo procedimiento, programa, utilidad o aplicación que se construye con el fin de atacar un sistema o un proceso.
- En sistemas de alta seguridad suelen instalarse antivirus con varios motores de análisis, cada uno de un proveedor de seguridad distinto.
- Clasificación general de malware:
  - Virus
  - Ransonware
  - Gusanos o worms
  - Caballos de troya o troyanos
  - Puertas falsas, traseras o backdoor
  - Spyware
  - Adware
  - Spam

3.2.4 ATAQUES CON SOFTWARE MALICIOSO

- **VIRUS**: se componen de una secuencia de instrucciones ejecutables con capacidad de autorréplica parasitando otras secuencias. Debe tenerse en cuenta que un virus no es un programa por sí solo: necesita el concurso de otro programa para llevar a cabo la infección. El principal objetivo de un virus es autorreplicarse, sin embargo, se le suele añadir otras funciones destructivas.
- **RANSONWARE**: es un tipo de programa dañino que restringe el acceso a determinadas partes o archivos del sistema infectado, y pide un rescate económico a cambio de quitar esta restricción. Algunos tipos de ransomware cifran los archivos del SO inutilizando el dispositivo y coaccionando al usuario a pagar el rescate.
- **GUSANOS O WORMS**: son programas independientes con autonomía de funcionamiento, capacidad de autorréplica y que actúan en entornos de red explotando alguna vulnerabilidad de algún protocolo o servicio. Su propósito principal es expandirse por los sistemas de la red y causar un ataque de denegación de servicio.

3.2.4 ATAQUES CON SOFTWARE MALICIOSO

- **TROYANOS**: son fragmentos de código que se esconden en el interior de un archivo con apariencia inofensiva. Un troyano es incapaz de replicarse: para reproducirse requiere el concurso de la actividad de un usuario. Su funcionamiento se basa en la ejecución del programa anfitrión, ejecutado por el usuario casi siempre por engaño, que activa el troyano.
- **BACKDOORS**: su objetivo es ofrecer un modo de acceso al sistema que esquiva las medidas de seguridad dejando puertos activos abiertos que actúan como servicios a las órdenes del atacante que actúa desde el otro lado de la red como un cliente de ese servicio.
- **SPYWARE**: es un software que se infiltra en el sistema con objeto de espiar las actividades de los usuarios, lo que constituye una información muy valiosa para el atacante.
- **ADWARE**: integra publicidad no deseada en las aplicaciones de los usuarios.
- **SPAM**: consiste en la recepción masiva de correo electrónico no deseado.

3.2.4 ATAQUES CON SOFTWARE MALICIOSO

- El malware establece su objetivo de ataque en el sistema en algunos lugares especialmente vulnerables (Targets de ataque).
- Las vulnerabilidades más buscadas por el malware son las que permiten escalar privilegios, las que permiten un ataque de denegación de servicios (DoS) y las que otorgan privilegios de Administrador o root. Estas vulnerabilidades se pueden generar tanto en el SO como en el software de aplicación.
- El atacante explota la vulnerabilidad mediante un exploit.
- La mayor parte de los troyanos y otros malware generan vulnerabilidades en los sistemas por lo que incrementan los riesgos de ataque del sistema desde el exterior, con independencia de los daños que puedan causar sus propias actividades maliciosas.

3.2.5 SEGURIDAD EN LA CONEXIÓN DE REDES PÚBLICAS

- Cuando un equipo realiza una conexión a una red pública aumenta el riesgo debido a que, aunque las vulnerabilidades permanecen inalteradas por el hecho de realizar la conexión, se incrementan notablemente las amenazas por el inmenso número de posibles ataques.
- Los riesgos más comunes en las conexiones a redes públicas son los siguientes:
  - El cortafuegos podría no estar configurado correctamente o puede que no proporcione suficiente protección.
  - Las transmisiones de información sobre seguridad (usuario y contraseña) no estén cifradas.
  - Las conexiones telnet o ftp, que no son cifradas.
  - Los hackers pueden obtener información sensibles en los foros, mailing-list…
  - Sesiones abiertas en servidores de chat (IRC)
  - Ataques de denegación de servicio.

3.2.5 SEGURIDAD EN LA CONEXIÓN DE REDES PÚBLICAS

- Estos riesgos se atenúan integrando en el plan de seguridad contramedidas como las siguientes:
  - Disponer de un antivirus de calidad y actualizado. En servidores deben instalarse antivirus con varios motores de análisis.
  - Tener siempre activado y bien configurado el cortafuegos.
  - Integrar el antivirus en una suite de seguridad que provea otros servidores de seguridad con antispam, antiphising y detección de vulnerabilidades.
  - Proteger las conexiones mediante cifrado. Por ejemplo sustituyendo http por https.
  - Utilización de redes privadas virtuales VPN.
  - Validar las conexiones remotas realizadas mediante robustos sistemas de autenticación.

3.3 SEGURIDAD EN LA RED CORPORATIVA

- Asegurarse un equipo es un logro importante que contribuye enormemente a la seguridad de una organización, pero no es suficiente.
- Los sistemas informáticos, cada vez más, son distribuidos de modo que las aplicaciones se encuentran repartidas entre varios sistemas conectados en red.
- Por tanto, la seguridad debe extenderse también a los protocolos de red y a los procedimientos de interconexión e intercambio de datos.
- Esto hace que haya elementos de seguridad específicos cuando se trata de proteger la red corporativa.

3.3.1 LA SEGURIDAD Y LAS VULNERABILIDADES EN REDES TCP/IP

- Las amenazas más frecuentes sobre los recursos de comunicaciones se agrupan en los siguientes cuatro tipos:
  - **INTERRUPCIÓN**: Integra los ataques de denegación de servicio, lo que produce una falta de disponibilidad.
  - **INTERCEPTACIÓN**: El atacante consigue hacer una copia de la información a la que no debería tener acceso, lo que produce una falta de privacidad.
  - **MODIFICACIÓN**: Una vez interceptado el mensaje, este puede ser modificado y reenviado al receptor suplantando al mensaje original, lo que ataca a la integridad.
  - **GENERACIÓN, CREACIÓN o FABRICACIÓN:** el atacante fabrica un mensaje que envía al receptor suplantándole, lo que agrede la autenticidad.

3.1 LA SEGURIDAD ACTIVA EN LOS SISTEMAS

VULNERABILIDADES DE LA CAPA DE RED TCP/IP (niveles 1 y 2 de OSI)

- En el nivel físico, la primera vulnerabilidad es la posibilidad de acceso físico al cuarto de telecomunicaciones, al cableado o a los equipos que intervienen en la comunicación, por ejemplo, ataques sobre los cables de datos, desvío del cableado o intercepción de las comunicaciones, lo que genera problemas asociados a la confidencialidad y al control de acceso.
- Para asegurar la capa de Red se tiene que considerar:
  - La confidencialidad: los datos solo han de estar disponibles para las personas autorizadas.
  - La autenticidad: debe verificarse la identidad digital de los agentes.
  - La integridad: debe comprobarse la exactitud de la información frente a alteraciones, pérdidas o destrucción de datos.
- Por tanto, se generan problemas de suplantación de mensajes y de direcciones físicas, alteración del control de acceso al medio mediante sniffers no autorizados y posibilidad de ataque mediante exploits contra los adaptadores de red.

3.1 LA SEGURIDAD ACTIVA EN LOS SISTEMAS

VULNERABILIDADES DE LA CAPA DE INTERNET TCP/IP (nivel 3 de OSI)

- El principal problema en este nivel es el de las escuchas no autorizadas de paquetes de nivel 3 (paquetes IP).
- Un segundo problema es el de la suplantación de direcciones IP, ya que IP carece de posibilidades de autenticación: para hacerlo requiere el concurso de protocolos de otras capas. Esto permite que se puedan robar sesiones de nivel superior, como TCP/IP.
- Un tercer ataque reside en el envenenamiento de las tablas de caché de ARP, que permiten la suplantación de las direcciones MAC utilizadas en el nivel 2.

3.1 LA SEGURIDAD ACTIVA EN LOS SISTEMAS

VULNERABILIDADES DE LA CAPA DE TRANSPORTE TCP/IP (nivel 4 de OSI)

- Los principales problemas en este nivel se asocian con la búsqueda e interceptación de puertos TCP y UDP.
- La apertura de puertos indiscriminada a su falta de protección en el cortafuegos corporativo, también puede producir la delación de los servicios ofrecidos que quedarán más expuestos al hacerlos públicos.
- La búsqueda de puertos abiertos suelen hacerse mediante utilidades de escaneo de la red.
- Aunque estos servicios estén protegidos mediante un mecanismo de autenticación, al hacerlos públicos, se prestan a ataques de fuerza bruta.

3.1 LA SEGURIDAD ACTIVA EN LOS SISTEMAS

VULNERABILIDADES DE LA CAPA DE APLICACIÓN TCP/IP (niv. 5 a 7 de OSI)

- Los niveles superiores se prestan a problemas asociados a los servicios de red y a la autenticación de datos, por lo que su protección también exige herramientas de muy alto nivel.
- Entre los problemas más comunes se encuentran los siguientes:
  - Deficiencias en los servicios de nombres de dominio.
  - Envenenamiento de las cachés del DNS.
  - Suplantación del servidor DNS.
  - Inseguridad de protocolos no cifrados que transportan contraseñas, como telnet o ftp.
  - Vulnerabilidades específicas del protocolo http, asociadas a las construcción de los URL, por ejemplo, en los ataques de inyección de código.

3.3.2 EL ATAQUE A UNA RED TCP/IP

ATAQUE DE INGENIERÍA SOCIAL, WEB Y WHOIS

- Un ataque de ingeniería social consiste en persuadir a los usuarios para que ejecuten acciones o revelan la información que el atacante necesita para comprometer la red.
- Sutilmente, el atacante puede deducir información sobre el acceso del usuario del target mediante la utilización de fechas, aniversarios, nombres de personas…
- Por eso, estos elementos nunca deben constituirse o formar parte de contraseñas.
- El análisis de una sede web puede proporcionar también mucha información a un atacante: direcciones de correo, organización corporativa…
- El servicio WHOIS, que es un protocolo TCP basado en petición/respuesta que se utiliza para efectuar consultas en una base de datos que permite determinar el propietario de un nombre de dominio o una dirección IP en Internet, por lo que también puede proporcionar información valiosa para el atacante.

3.3.2 EL ATAQUE A UNA RED TCP/IP

ATAQUE DE DENEGACIÓN DE SERVICIO

- El objetivo principal de un ataque de denegación de servicios (DoS) es impedir el uso legítimo del sistema atacado por parte de los usuarios autorizados.
- Suele producirse porque el atacante provoca un excesivo consumo de recursos del servidor, que impide que estos recursos lleguen a los usuarios legítimos.

3.3.2 EL ATAQUE A UNA RED TCP/IP

ATAQUE DE DENEGACIÓN DE SERVICIO

- Frecuentemente, el atacante no se esconde detrás de un único sistema, sino de detrás de toda una red de atacantes (botnet o red zombie) compuesta de sistemas infectados con troyanos especializados en el ataque y coordinados por el hacker que los dirige.
- En este caso, el ataque se denomina DDoS o ataque de denegación de servicio distribuido.
- La defensa de un ataque DoS se realiza bloqueando la dirección IP del atacante, de modo que este no consuma recursos.
- La defensa del ataque DdoS ya no es tan fácil puesto que el número de sistemas que atacan simultáneamente es innumerable.

3.3.2 EL ATAQUE A UNA RED TCP/IP

CRAKING DE CONTRASEÑAS, MAIL BOMBING Y SPAMING

- Es el proceso por el que se descubre la contraseña de un usuario en un sistema atacado.
- El atacante tendrá mucho interés en que ese usuario precisamente sea privilegiado, típicamente Administrador o root. Esta es la razón por la que deshabilitar o renombrar estas cuentas levantará una barrera más al atacante, que tendrá que descubrir no solo la contraseña sino el identificador de la cuenta privilegiada.
- Hay dos métodos fundamentales para el crakeo de contraseñas:
  - **Ataque por diccionario**. Consiste en efectuar un ataque ordenado utilizando palabras de un diccionario hasta encontrar la contraseña buscada, lo que exige que esta esté contenida en el diccionario. Impidiendo que las contraseñas estén en cualquier diccionario, derribaremos el éxito de este ataque.
  - **Ataque por fuerza bruta.** Se trata de realizar todas las combinaciones posibles de un conjunto de caracteres y de una longitud máxima, confiando en que la contraseña buscada se halle en alguna de estas combinaciones. Este ataque se dificulta en la medida en que se exija que las contraseñas sean suficientemente largas y tengan una gran variedad de símbolos (letras mayúsculas, minúsculas, números y caracteres especiales).

3.3.2 EL ATAQUE A UNA RED TCP/IP

CRAKING DE CONTRASEÑAS, MAIL BOMBING Y SPAMING

- El ataque de **mail bombing** consiste en enviar muchas veces el mismo mensaje a un usuario provocando ataques DoS por desbordamiento del buzón.
- En cambio, el ataque de **mail spamming** se orienta a enviar mensajes no deseados a muchos buzones distintos, provocando no solo la pérdida de recursos en los buzones de destino sino también problemas en el servidor de correo que emite los mensajes.
- Por tanto, el elemento más perjudicado con **mail bombing es** el cliente mientras que en el caso de **mail spamming** el más perjudicado es el servidor, aunque no se este el objetivo primordial del spammer.

3.3.2 EL ATAQUE A UNA RED TCP/IP

ESCANEO DE PUERTOS Y SNIFFERS

- El escaneo de puertos es un procedimiento ampliamente utilizado por los hackers para averiguar qué puertos están abiertos en el target objetivo de su ataque.
- Una vez conocidos los puertos abiertos, el hacker intentará buscar vulnerabilidades en los servicios que se hallan detrás de los puertos abiertos.
- Esta es la razón por la que conviene tener el sistema y las aplicaciones actualizadas y que, por tanto, tengan sus vulnerabilidades conocidas corregidas.
- Algunos cortafuegos detectan las actividades de rastreo de los escáneres de puertos.
- Los cortafuegos más avanzados pueden incluso, presentar resultados ficticios al escáner de puertos, de modo que este confunda al hacker que lo emplea.
- Los sniffers o escuchadores de red operan activando la interfaz de red del sistema sobre el que se ejecutan en modo promiscuo.
- En este modo de configuración de la tarjeta de red, el sniffer almacenará en un fichero de log todo el tráfico que circule por el punto de red en el que se conecta el adaptador, sea él o no el destinatario del tráfico.

3.3.2 EL ATAQUE A UNA RED TCP/IP

ESCANEO DE PUERTOS Y SNIFFERS

- La utilización de un sniffer permite la obtención de una gran cantidad de información sensible enviada sin cifrar: nombres de usuario, contraseñas, direcciones de correo electrónico…
- El análisis de la información transmitida permite a su vez extraer relaciones entre los equipos y así poder intuir una posible topología de la red, lo que es una información muy relevante para el atacante.
- La condición necesaria para que un sniffer pueda recoger un tráfico amplio y variado es que este pase por el puerto de red del sistema en que se ejecute.
- Esto no ocurre en redes conmutadas ya que estas solo hacen pasar por el puerto el tráfico con origen y destino en el sistema.
- Sin embargo, si en vez de conmutadores se utilizan hubs, que son repetidores multipuertos, todos los puertos reciben todo el tráfico.
- Esta es la razón de que los hubs sean mucho más inseguros que los switches.
- En el caso de las redes conmutadas, los switches suelen implementar una función de mirroring entre puertos por la que el tráfico destinado o con origen en un puerto concreto es copiado también a otro en el que se conecta el sniffer, de este modo el escuchador puede recoger el tráfico de la red por ese puerto.

3.3.3 RIESGOS POTENCIALES EN LOS SERVICIOS DE RED

- Los clientes consumen los recursos de red en forma de servicios. Cada servicio lleva asociado un software que le proporciona soporte sobre el SO, por tanto, las vulnerabilidades de ese software pueden producir riesgos para ese servicio de red.
- Por otra parte, si el servicio no está correctamente configurado puede dejar abiertas posibilidades al atacante.
- Otros posibles problemas pueden venir de la apertura de puertos TCP o UDP no controladas, por los servicios de red gestionados mediante puertas traseras o por otro malware.
- Para hacer que un sistema sea más seguro hay que tender a que exhiba la "mínima superficie de exposición", que es un concepto que se acuña para describir que solo se deben instalar los servicios que realmente se utilicen. Ninguno más.

3.3.3 RIESGOS POTENCIALES EN LOS SERVICIOS DE RED

- Por ejemplo:
  - En el cortafuegos solo deben estar abiertos los puertos de los servicios que estén activos.
  - Solo deben activarse los servicios estrictamente necesarios.
  - Únicamente deben instalarse los servicios que vayan a ser activados.
  - Si hay posibilidad de elegir, es mejor utilizar un protocolo cifrado que su equivalente no cifrado.
  - Si se puede elegir y el servicio se presta a ello, es mejor utilizar un protocolo autenticado que otro que no admita autenticación.

3.3.6 SEGURIDAD EN REDES INALÁMBRICAS

- Si la seguridad en las redes con medios cableados es importante, no es comparable a la necesidad de seguridad cuando la red utiliza medios no guiados en donde la señal y, por tanto, la información puede llegar a todos los lugares dentro de su rango geográfico de radiación facilitando la posibilidad de escucha no autorizada de la red.
- Para resolver este problema se han desarrollado varios protocolos que cifran la información, autentican los clientes…
  - Protocolo WEP
  - Protocolo IEEE 802.11i y 802.11n
  - WPA y WPA2

3.3.6 SEGURIDAD EN REDES INALÁMBRICAS

PROTOCOLO WEP

- El primer protocolo de seguridad que se creó fue WEP (Wired Equivalen Privacy), que como su nombre indica fue un intento de hacer que el medio inalámbrico tuviera una seguridad semejante a la del cable.
- WEP utiliza claves para autenticar a los clientes y para cifrar sus conexiones.
- Para ello, debe establecer una cadena de caracteres que se asocia como una clave de punto de acceso (network key).
- Esta clave debe ser conocida exclusivamente por lo clientes del punto de acceso y, obviamente, por el punto de acceso.
- La misma clave servirá para cifrar las conexiones entre clientes y punto de acceso, y para que los clientes (las estaciones inalámbricas) se autentiquen en bits se consiguen romper fácilmente.

3.3.6 SEGURIDAD EN REDES INALÁMBRICAS

PROTOCOLO IEEE 802.11i y 802.11n

- 802.11i utiliza EAPoL (802.1x) para autenticar dispositivos y proporcionar dinámicamente a cada transmisión su propia clave.
- 802.1x es un método de acceso a la red en la que esta decide si el sistema que se conecta por un puerto tiene o no derecho a conectarse.
- 802.11i suele utilizar TKIP (Temporal Key Integrity Protocol) como sistema de gestión y generación de claves de cifrado, requiere autenticado recíproco entre el punto de acceso y el cliente.
- Puede utilizar AES como método de cifrado, que es de los más robustos.
- IEEE 802.11n es el protocolo de seguridad para redes inalámbricas que integra 802.11i además de otras extensiones de seguridad y que se ha reconocido internacionalmente como el estándar seguro por antonomasia para redes Wi-Fi.

3.3.6 SEGURIDAD EN REDES INALÁMBRICAS

WPA y WPA2

- Wi-Fi Protected Access (WPA) es un subconjunto del estándar 802.11i aprobado por la Wi-Fi Alliance que surge como una alternativa más segura WEP a quien desplaza, aunque no llega a ser tan seguro como 802.11i.
- La autenticación en WPA sigue el mismo mecanismo especificado en 802.11i (de hecho WPA es anterior cronológicamente a 802.11i).
- Básicamente se diferencian en que WPA cifra con RC4 mientras que 802.11i cifra AES, mucho más seguro.
- Existe una versión 2 de WPA mejorada denominada WPA2, que es compatible con WPA.

3.3.7 SEGURIDAD PERIMETRAL

- Seguridad perimetral, todos los sistemas que están en contacto tanto con la LAN interna como con Internet o la red externa.
- Estos equipos están especialmente sobreexpuestos por lo que requieren una exquisita atención por parte del administrador de seguridad.

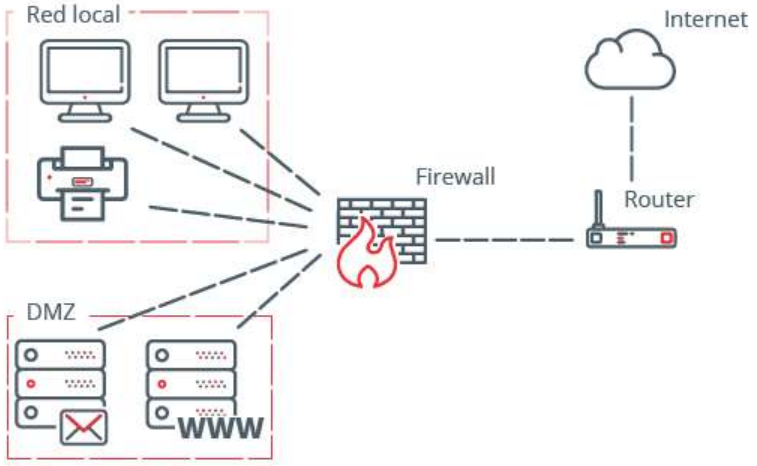
CONCEPTO DE IDS

- Un sistema de detección de intrusos (IDS) es aquel que detecta manipulaciones no deseadas en los sistemas o ataques malintencionados no detectados por los cortafuegos mediante el análisis del tráfico de red y la vigilancia de las actividades de los usuarios de red.
- Su operación se basa en la monitorización de eventos y la gestión posterior de alertas basadas en reglas.
- Existen 3 tipos básicos de IDS:
  - HIDS (Host IDS): un sistema que vigila un único sistema.
  - NIDS (Network IDS): un sistema que se basa en la red, detectando ataques que se hacen en la misma.
  - DIDS (Distributed IDS): un sistema basado en la arquitectura cliente-servidor que está compuesto por múltiples NIDS, que actúan como sensores centralizando la información de posibles ataques en una unidad central. Suele ser la estructura habitual de seguridad en redes VPN

3.3.7 SEGURIDAD PERIMETRAL

CONCEPTO DE DMZ O RED PERIMETRAL

- Una zona desmilitarizada es una **red aislada que se encuentra dentro de la red interna de la organización**.
- En ella se encuentran ubicados exclusivamente todos los recursos de la empresa que deben ser accesibles desde Internet, como el servidor web o de correo.
- Por lo general, una DMZ permite las conexiones procedentes tanto de Internet, como de la red local de la empresa donde están los equipos de los trabajadores, pero **las conexiones que van desde la DMZ a la red local, no están permitidas**.
- Esto se debe a que los servidores que son accesibles desde Internet son más susceptibles a sufrir un ataque que pueda comprometer su seguridad.



3.3.7 SEGURIDAD PERIMETRAL

ATAQUES INTERNOS Y EXTERNOS

- Uno de los mayores errores de seguridad es pensar que los ataques solo pueden venir de la red externa.
- La mayor parte de los ataques que sufre una organización vienen de su interior.
- En la red externa son más frecuentes los intentos de intrusión mientras que en la red interna hay que vigilar especialmente las fugas de información, la confidencialidad, las puertas trasera y las bombas lógicas.
- Los ataques externos van sobretodo encaminados a conseguir penetrar en algún sistema de la red interna desde donde proseguir el ataque al resto de la organización.

3.3.7 SEGURIDAD PERIMETRAL

PUNTOS DESTACABLES EN LA SEGURIDAD DE LA RED INTERNA

1. Antimalware y cortafuegos. Hay que llegar a un equilibrio entre los requisitos que necesitan los usuarios para realizar su trabajo y las limitaciones que se producirían con una defensa excesiva.
2. Realizar un enfoque multicapa (defensa en profundidad), sin descuidar ninguna de ellas.
3. Auditar constantemente cada uno de los niveles de defensa.
4. Subdividir la red en segmentos lógicos en conmutadores y routers mediante subnetting en el nivel 3 y mediante creación de VLANs en el nivel 2 y 3.
5. Cuidar la política de contraseñas y gestionar los protocolos de autenticación de usuarios.
6. Deshabilitar los usuarios o servicios de invitados y renombrar los identificadores de las cuentas de usuario de los administradores por defecto (Administrador, root).
7. Implementar componentes de seguridad perimetral.
8. Tener actualizados los sistemas y correctamente administrados.
9. Disponer de un Sistema de Detección de Intrusiones (IDS).

3.3.7 SEGURIDAD PERIMETRAL

PUNTOS DESTACABLES EN LA SEGURIDAD DE LA RED PERIMETRAL

1. La red perimetral es la parte de la red que están en contacto con el exterior y que, por tanto, sufre la máxima exposición al ataque.
2. Los principales problemas se centran en los puertos TCP o UDP.
3. La seguridad de la red perimetral es inútil si se descuida la seguridad de la red interna.
4. Los ataques con éxito a la red perimetral deterioran la credibilidad y el prestigio de la organización.

3.3.7 SEGURIDAD PERIMETRAL

TECNOLOGÍAS PARA LA SEGURIDAD PERIMETRAL

- Al diseñar la arquitectura de seguridad, el responsable de seguridad debe trabajar con el administrador de sistemas y redes.
- Las soluciones de seguridad se componen de normas y procedimientos, pero también son necesarios dispositivos físicos que organicen la red con una arquitectura determinada que provea los mecanismos de seguridad necesarios.
- Los dispositivos de red o sistemas (hardware o software) que constituyen soluciones de seguridad para uso del administrado de seguridad pueden ser:
  1. Routers
  2. Cortafuegos (firewalls)
  3. Sistemas de Detección de Intrusiones (IDS)
  4. Redes Privadas Virtuales (VPN)
  5. Software y servicios
  6. Zonas desmilitarizadas (DMZ) y subredes controladas (o apantalladas)