TEMA 5 SEGURIDAD ACTIVA EN EL SISTEMA

1. INTRODUCCIÓN A LA SEGURIDAD DEL SISTEMA

Seguridad activa: conjunto de medidas que previenen o intentan evitar los daños en el sistema informático.

Se trata de estudiar los **mecanismos de protección** que podemos utilizar en nuestro equipo informático para evitar accesos indeseados de **intrusos (personas o programas informáticos).**

Aprenderemos a:

Mejorar la seguridad en el acceso al ordenador mediante el uso de contraseñas en la BIOS y en el gestor de arranque.
Impedir la carga de un sistema operativo desde dispositivos extraíbles, memoria externa USB, CD/DVD…
Configurar la contraseña de las cuentas.
Mejorar la seguridad ante los ataques definiendo políticas de contraseñas y mecanismos de autenticación.
Auditar todas las acciones anteriores.
Estudiar las vulnerabilidades de nuestro sistema.
Conocer los procesos que se ejecutan en nuestro sistema y su utilidad.

Para ello debemos conocer el software que vulnera la seguridad del sistema:

Atacantes
Tipos de ataques
Malware

2. SOFTWARE QUE VULNERA LA SEGURIDAD DEL SISTEMA

Malware – software malicioso

Exploit

2.1 TIPOS DE ATAQUES

Ataques de acceso, modificación, denegación de servicio o refutación

Ataques contra la confidencialidad – contra la integridad – contra la disponibilidad – contra la responsabilidad

Los ***ataques*** pueden ocurrir a través de medios técnicos como **herramientas diseñadas para ataques** o **mediante la exploración de vulnerabilidades** en un sistema de cómputo, o pueden presentarse a través de una **ingeniería social** (utilización de medios no técnicos para obtener acceso no autorizado).

Lo ataques contra la información en formato electrónico tienen otra característica interesante, aunque la información puede ser copiada, normalmente no es robada. **Copiar es delito**.

2.1.1 ATAQUES DE ACCESO

Un ataque de acceso es un intento de obtener información que el atacante no está autorizado a ver

Control de acceso como defensa

Este ataque puede ocurrir en cualquier lugar en el que la información esté depositada, o se pueden presentar durante la transmisión.

Este tipo de ataque está **dirigido contra la confidencialidad de la información**.

Fisgoneo

Hurgar entre los archivos de información con la esperanza de hallar algo interesante.

Escucha furtiva

Cuando alguien escucha una conversación de la que no forma parte, se dice que escucha furtivamente.
Para obtener el acceso no autorizado a la información, un atacante debe colocarse en un sitio donde sea probable que circule información de interés.
La introducción de las redes inalámbricas ha incrementado la oportunidad de escuchar furtivamente.

Interceptación

A diferencia de la escucha furtiva, la interceptación es un ataque activo contra la información. Cuando un atacante intercepta información, se coloca él mismo en la ruta de la información y la

captura antes de que alcance su destino. Después de examinar la información el atacante puede permitir que la información continúe hasta su destino, o no hacerlo.

COMO SE CONSUMAN LOS ATAQUES DE ACCESO

Los ataques de acceso (todos en general, no solo los de acceso) asumen diferentes formas, dependiendo si la información se encuentra almacenada en papel o de manera electrónica en un dispositivo de cómputo.

Información en papel:

Acceso físico a dicho papel (archivadores, cajones, impresoras, fax, papeleras, basura, archivos muertos…)

Información electrónica:

La información electrónica puede estar almacenada en ordenadores de escritorio, servidores, ordenadores portátiles, CD, DVD, cintas,….
La información electrónica también puede ser atacada cuando se mueve por la red para ser transmitida de un equipo a otro.
Rastreador – Analizador de tráfico (sniffer): computadora configurada para capturar todo el tráfico de la red (no solo el que está dirigido a dicha computadora).

2.1.2 ATAQUES DE MODIFICACIÓN

Un ataque de modificación es un intento de modificar la información que un atacante no está autorizado a modificar.

Cifrado y firma digital como defensa

Este ataque puede ocurrir donde quiera que radique la información (información almacenada). También puede intentarse en contra de la información en transito.

Este tipo de ataque es **en contra de la integridad de la información**.

Cambios

Un tipo de ataque de modificación es el cambio de la información existente. La información ya existía en la organización, pero ahora es incorrecta.
Los ataques de cambios pueden ser dirigidos a información confidencial o información pública.

Inserción

Otro tipo de ataque de modificación es la inserción de información. Cuando se realiza un ataque de inserción se agrega información que no existía con anterioridad.
Este tipo de ataque puede ser montado en contra de información histórica o de información sobre la que todavía se harán modificaciones futuras.

Eliminación

Un ataque de eliminación consiste en el borrado de la información existente. Esto puede sobre un registro histórico o sobre un registro que todavía podría sufrir modificaciones.

COMO SE CONSUMAN LOS ATAQUES DE MODIFICACIÓN

Los ataques de modificación asumen diferentes formas, dependiendo si la información se encuentra almacenada en papel o de manera electrónica en un dispositivo de cómputo.

Información en papel:

> Los registros de papel pueden ser difíciles de modificar sin que los cambios sean detectados y requieren tener acceso físico a los documentos.

Información electrónica:

> La modificación de la información en formato electrónico es mucho más sencilla.
> Suponiendo que el atacante tenga acceso a los archivos, pueden hacerse modificaciones dejando evidencias mínimas.
> Si el atacante no tiene acceso autorizado a los archivos, primero tendría que incrementar su acceso al sistema o eliminar los permisos sobre el archivo (ataque de acceso).
> En las bases de datos se suelen numerar las transacciones para detectar este tipo de ataques.
> Es más difícil montar con éxito un ataque de modificación de la información en tránsito. La mejor forma de hacer esto sería ejecutar primero un ataque de intercepción contra el tráfico en el que se esté interesado y, posteriormente, modificar la información antes de pasarlo a su destino.

2.1.3 ATAQUES DE DENEGACIÓN DE SERVICIO

Los ataques de denegación de servicio (DoS, Denial-of-Service) son ataques que niegan el uso de los recursos a los usuarios legítimos del sistema, de la información o de las capacidades

Cuotas y control de acceso como defensa

Por lo general los ataques de DoS no permiten que el atacante tenga acceso o modifique la información en el sistema de cómputo o en el mundo físico.

Los ataques de DoS no son otra cosa que vandalismo.

Denegación de acceso a la información

> Un ataque de denegación de servicio en contra de la información provoca que dicha información no esté disponible.
> Esto puede ser cambiado por la destrucción de la información o por el cambio de la misma hasta dejarla de una forma no utilizable.
> Esta situación puede ser causada si la información aun existe pero ha sido removida a una ubicación inaccesible.

Denegación de acceso a las aplicaciones

> Otro tipo de ataque de DoS está dirigido a la aplicación que manipula o exhibe la información.

Este es normalmente un ataque en contra del sistema de cómputo que ejecuta la aplicación. Si la aplicación no está disponible, la organización no puede realizar las tareas que son desempeñadas por esa aplicación.

Denegación de acceso a los sistemas

Este es un tipo común de ataque de DoS para derribar sistemas de cómputo.
En este tipo de ataque el sistema, junto con todas las aplicaciones que corren en el mismo y toda la información que se encuentra almacenada en él, dejan de estar disponibles.

Denegación de acceso a las comunicaciones

Los ataques de DoS en contra de las comunicaciones se han realizado durante muchos años.
Abarca desde cortar un alambre hasta inundar redes con tráfico excesivo.
Aquí el objetivo es el medio de comunicación por sí mismo. Normalmente, los sistemas y la información permanecen ilesos, pero la carencia de comunicaciones evita el acceso a los sistemas y a la información.

COMO SE CONSUMAN LOS ATAQUES DE DENEGACIÓN DE SERVICIO

Los ataques de DoS son principalmente ataques en contra de redes y sistemas informáticos. Esto no quiere decir que no existan ataques de DoS en contra de la información en papel, solo que es mucho mas fácil dirigir un ataque de DoS en el mundo electrónico.

DoS eliminando la información y todas sus copias.
DoS modificando la información (ej, encriptandola).
DoS bloqueando, robando, … las máquinas que ofrecen el servicio (explotando las vulnerabilidades de los sistemas).
DoS bloqueando las aplicaciones que ofrecen el servicio (explotando las vulnerabilidades de las aplicaciones).
DoS bloqueando, saturando, cortando… el sistema de comunicaciones.

No todos los ataques de DoS son **intencionados**; los **accidentes** juegan un papel importante en este tipo de problemas. (Obras, Climatología, pruebas de software, uso indebido del sistema,…).

2.1.4 ATAQUES DE ATAQUES DE REFUTACIÓN

La refutación es un ataque en contra de la responsabilidad de la información.

Certificados digitales como defensa

La refutación es un intento de proporcionar información falsa o de negar que una transacción o evento reales hubieran ocurrido.

Simulación

La simulación es un intento de actuar como, o de hacerse pasar, por alguien o por algún otro sistema.
Este ataque puede ocurrir en la comunicación personal, en transacciones, o en comunicaciones entre sistemas.

Denegación de un evento

La denegación de un evento es simplemente negar que la acción se haya realizado como fue registrada.
Ej. Hacemos una compra con la tarjeta de crédito. Cuando llega la cuenta, la persona le dice a la compañía de tarjetas de crédito que nunca hizo esa compra.

COMO CONSUMAR LOS ATAQUES DE REFUTACIÓN

Los ataques de refutación pueden efectuarse en contra de la información tanto en forma física como electrónica.

La dificultad del ataque depende de las precauciones que hayan sido tomadas por la organización.

Información en papel:

Falsificación de la firma.
Notaría, Registro de la propiedad...

Información electrónica:

La información electrónica puede ser más susceptible a un ataque de refutación que la información en forma física.
Pueden crearse documentos electrónicos y enviarse a otros con pocas pruebas, o ninguna, de la identidad del remitente.
Ciberbullying, ciberacoso, e-acoso
Lo mismo es cierto para la información enviada desde sistemas de computo. Modificando la IP, cualquier sistema de cómputo puede hacerse pasar por cualquier otro.
Spam, correo basura (“anónimo”, falseando el origen, forzando a equipos a enviarlo).

La denegación de un evento en el mundo electrónico es mucho más fácil que en el mundo físico. A menos que el documento esté firmado con una firma digital, no hay nada que pruebe que el documento fue aceptado por un individuo.

Incluso habiendo firmas digitales, pondríamos decir que fueron robadas o adivinada su contraseña… Lo mismo pasa con las transacciones de la tarjeta de crédito.

2.2 HACKERS

No se trata de aprender a ser un hacker, sino de conocer sus motivaciones y sus técnicas para saber cómo pondrían atacar y utilizar nuestros sistemas.

Hackear

Hacker: individuo que descubre y/o utiliza las vulnerabilidades de nuestros sistemas.

En el pasado hacker designaba al individuo que podía hacer que las computadoras funcionaran.

2.2.1 MOTIVACIONES DE UN HACKER

Retos

La motivación original para allanar sistemas de computo era simplemente el reto que suponía hacerlo.
Esta sigue siendo aún la motivación más común para los hackers.
La motivación del reto se asocia con los hackers sin objetivos específicos, invaden sistemas por diversión o sin que les importe en realidad qué sistemas comprometen.
Hacktivismo

Codicia

La codicia es una de las motivaciones más antiguas para la actividad delictiva conocida.
En el caso de los hackers, la motivación incluye algún deseo de ganar, ya sea dinero, bienes, servicios o información.
Señalar la dificultad para identificar, arrestar y condenar a un hacker.

Propósito malintencionado

La motivación final para los hackers con propósitos malintencionados es el vandalismo o cometer actos malintencionados.
A este tipo de hackers no les interesa controlar el sistema sino causar daños denegando o modificando el servicio.

2.2.2 TÉCNICAS HISTÓRICAS

Recursos compartidos mal configurados

Cuando fue creado Internet, la idea original fue compartir abiertamente la información y permitir la colaboración entre instituciones de investigación.
En el caso de los sistemas Unix, se utilizó el sistema de archivos de red (NFS, Network File System).
El NFS permite que una computadora monte las unidades de otra computadora a través de una red.
Esto puede hacerse a través de Internet del mismo modo que puede hacerse a través de una LAN.
La **compartición abierta** de archivos puede considerarse un serio error de configuración en lugar de una vulnerabilidad.

Contraseñas deficientes

Quizás el método más común utilizado por los hackers para introducirse en los sistemas es a través de contraseñas endebles.
Las contraseñas o passwords siguen siendo la forma más común de autenticación o validación en uso. Puesto que las contraseñas son un método de autenticación predeterminado en la mayor parte de los sistemas, utilizarlas no provoca un costo adicional. Un beneficio adicional de utilizar contraseñas es que los usuarios comprenden cómo emplearlas. Por desgracia, muchos usuarios no entienden como elegir contraseñas efectivas. Esto nos deja con el problema de que muchas contraseñas son cortas y fáciles de adivinar.

Las contraseñas cortas permiten que el hacker las averigüe utilizando la fuerza bruta.
El otro tipo de contraseña débil es que es fácil de adivinar.

Fallos de programación

Los hackers se han aprovechado muchas veces de fallos de programación.
Estos incluyen cosas como dejar una puerta trasera en un programa para accesos posteriores.

Ingeniería social

La ingeniería social es el uso de medios no técnicos para obtener el acceso no autorizado a la información o a los sistemas.

Desbordamiento de Buffer

Los desbordamientos de buffer son un tipo de fallo de programación explotado por los hackers.
Son más difíciles de descubrir que las malas contraseñas o los errores de configuración importantes; es preciso tener bastante habilidad para encontrar y explotar un desbordamiento de búfer. Pero también puede ser que quien los encuentra publique su hallazgo para que otros lo usen…
Son especialmente peligrosos porque tienden a permitir que los hackers ejecuten cualquier comando que deseen en el sistema objeto.

¿Qué es un desbordamiento de buffer?
En el caso de los desbordamientos de buffer, la parte de la memoria que se desborda se denomina pila o stack, y es, en particular, la dirección de retorno de la función que se ejecutará a continuación.
La pila controla la comunicación entre los programas, y dice a los sistemas operativos que código ejecutar cuando una parte de un programa (o función) haya completado su tarea. La pila también almacena variables locales a la función.
Cuando el hacker explota el desbordamiento de buffer coloca instrucciones (que le convienen) en variables locales que se almacenan en la pila. La información colocada en la variable local es suficientemente extensa para colocar una instrucción en la pila y sobrescribir la dirección de retorno para señalar hacia una nueva instrucción.

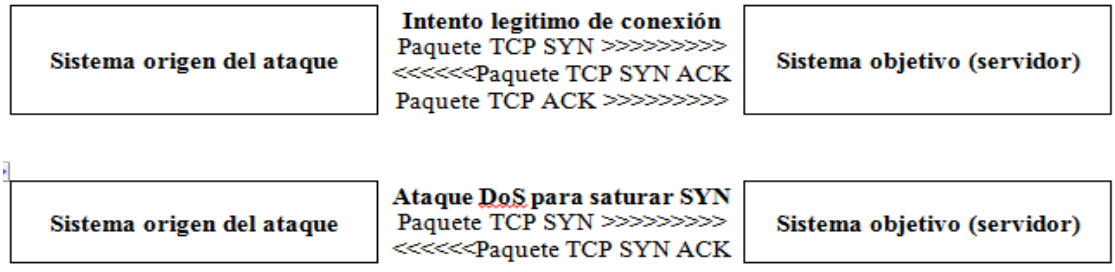
¿Por qué ocurren los desbordamientos de buffer?
Los desbordamientos de buffer se presentan muy frecuentemente como un fallo en la aplicación que copia los datos del usuario en otra variable sin verificar la cantidad de datos que está copiando.

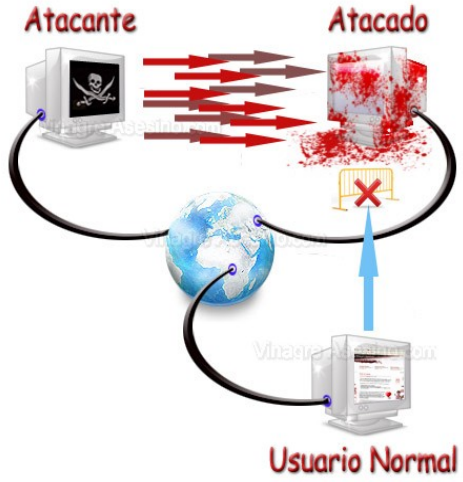
Es mucho más fácil solucionar un desbordamiento de búfer cuando se escribe el programa que descubrirlo a posteriori.

Denegación de servicio (DoS)

Los ataques de denegación de servicio (DoS) son sencillamente actos malintencionados para denegar el acceso a un sistema, red, aplicación o información, al usuario legítimo.
Los ataques de DoS pueden tomar muchas formas y pueden ser lanzados tanto desde sistemas individuales como de sistemas múltiples.
Dejando a un lado los ataques físicos de DoS.
Puesto que el atacante no está intentando obtener acceso al sistema objetivo, en un ataque de DoS se suelen utilizar direcciones que se obtuvieron fisgoneando (o que fueron falsificadas) manipulando la dirección IP origen.
La mayor parte de los ataques de DoS no requieren que el tráfico regrese hacia el sistema de inicio del hacker para ser efectivos.

Ataques de denegación de servicio desde una fuente simple:





Ataques de denegación de servicio distribuido (DDoS)

Los ataques de DoS distribuidos (DDoS) son simplemente ataques de DoS que se originan desde un gran número de sistemas. Los ataques de DDoS suelen ser controlados desde un solo sistema maestro y por un solo hacker.

Estas herramientas tienen una arquitectura a tres niveles. Un hacker negocia un proceso maestro o de servidor que ha sido colocado en un sistema comprometido. El maestro negocia con procesos esclavos o clientes que hayan sido instalados en otros sistemas comprometidos. Los sistemas esclavos (zombis) efectúan directamente el ataque contra el sistema objetivo.

2.2.3 TÉCNICAS AVANZADAS

Requieren el conocimiento detallado de sistemas y redes

Hijacking Sniff*er* Spoofing Phishing

Muchos de los ataques que se ven en la actualidad son ejecutados por “niños de scripts”, es decir, individuos que encuentran en Internet un script de explotación y lo disparan contra cualquier sistema que puedan hallar.

En cambio hay otras técnicas que requieren un conocimiento más detallado de sistemas, redes y de los sistemas objetivo.

Rastreo de redes

Con la finalidad de rastrear el tráfico en un ambiente conmutado, el hacker debe hacer una de dos cosas:

1. Convencer al conmutador (switch) de que el tráfico interesante debería dirigirse hacia el rastreador.
2. Provocar que el conmutador envíe todo el tráfico a todos los puertos.

Si se puede crear cualquiera de estas dos condiciones, el rastreador puede examinar el tráfico de interés y así proporcionar al hacker la información deseada.

Redireccionamiento del tráfico

Métodos utilizados para provocar que el conmutador envíe tráfico hacia el rastreador.

Falsificación de ARP

Duplicación de MAC
Falsificación de DNS

Enviar todo el tráfico a todos los puertos
El hacker intentará que el switch trabaje como un hub (concentrador) saturando la memoria del conmutador.

Falsificación de direcciones IP

Explotan una vulnerabilidad en el número de secuencia inicial (ISN Initial Sequence Number) que contiene el encabezado de los paquetes TCP para reconocer los paquetes de una conexión.

Detalles de un ataque de falsificación de IP
El hacker falsifica la IP origen y solicita una conexión al sistema objetivo, este le envía un paquete SYN ACK que contiene el ISN del objetivo,… (Pendiente de describir mejor).
Spoofing

Utilización de falsificación de IP en el mundo real
Cuando rlogin o rsh está configurado en un sistema, la dirección IP fuente es un importante componente para determinar quien tiene permiso de utilizar un servicio. Los anfitriones remotos que serán aceptados en tales conexiones se denominan fiables. Si podemos utilizar el falseamiento de IP para engañar a un objetivo haciendo que piense que provenimos de un sistema fiable, quizá podamos comprometer al sistema con éxito.

2.2.4 IDENTIFICACIÓN DE CÓDIGO MALINTENCIONADO

El código malintencionado continúa siendo un gran problema de seguridad para la mayoría de las organizaciones y usuarios de sistemas informáticos.

Malware: Virus – Troyanos - Gusanos

El código malintencionado cubre tres diferentes tipos de programas:

Virus

Los virus de computadora son trozos de programas que van embebidos en otros programas ejecutables.

Cuando el programa al que un virus está vinculado se ejecuta, el código del virus también se ejecuta y realiza sus acciones. Estas acciones normalmente incluyen difundirse a sí mismo hacia otros programas o discos. Algunos virus son malintencionados y eliminan archivos o provocan que los sistemas queden inutilizados. Otros virus no realizan ningún acto malintencionado, excepto extenderse ellos mismos hacia otros sistemas.

Troyanos

Del mismo modo que los griegos utilizaron un regalo para ocultar la evidencia de un ataque, un programa caballo de Troya oculta su naturaleza maliciosa detrás de la fachada de algo útil o interesante.

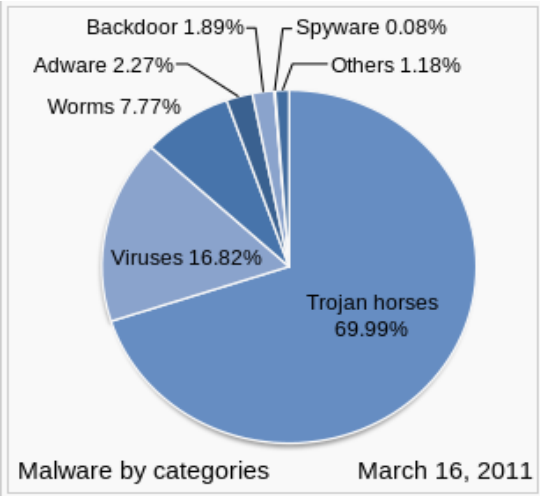
Un caballo de Troya es un programa completo o autocontenido que está diseñado para realizar algún tipo de acción malintencionada. Se presenta a si mismo como algo en que el usuario puede tener algún interés, como una nueva capacidad o un correo electrónico que el usuario quiera leer.

Gusanos

Un gusano es un programa que se arrastra de sistema en sistema sin ninguna ayuda de sus víctimas. El gusano se extiende por sus propios medios y también se reproduce por sí mismo. Todo lo que se requiere es que el creador del gusano lo active.

Híbridos

Otra capacidad es la combinación de dos tipos de código malintencionado en un solo programa. En otras palabras, estamos comenzando a ver programas que actúan como gusanos y como caballos de Troya.



Malware por categorías el 16 de marzo de 2011.

2.2.5 MÉTODOS DE LOS HACKERS SIN OBJETIVOS ESPECÍFICOS

Objetivos

No tienen ninguno, al menos previamente.

Los hackers sin objetivo específico son individuos que no están buscando el acceso a organizaciones o información en particular, sino que buscan cualquier sistema que puedan comprometer.

Reconocimiento para el ataque

Reconocimiento de Internet (rastreo sigiloso)

Los hackers sin objetivo específico realizan un rastreo sigiloso o rastreo medio de IP contra un intervalo de direcciones para identificar sistemas susceptibles de ser atacados.
Un **rastreo sigiloso** es un intento para identificar sistemas dentro de un intervalo de dirección. También puede identificar los servicios que ofrece el sistema identificado, dependiendo de cómo se realiza el rastreo.
El rastreo sigiloso puede ser utilizado en conjunto con un **barrido ping (ping sweep)** del intervalo de dirección. Un barrido ping es simplemente un intento por hacer ping en cada dirección y ver si se recibe una respuesta.

Reconocimiento telefónico

Wardialing ("marcación de combate") es el método que utilizan los hackers par identificar sistemas que tienen módems que responden a llamadas entrantes.

Reconocimiento inalámbrico (warchalking)

Warddriving: moverse en los alrededores con una computadora y un adptador de red inalámbrica con el propósito expreso de identificar redes inalámbricas; GPS para registrar las ubicaciones; warchalking: marcas en el suelo o en los edificios; …
Una vez que la red inalámbrica es identificada, el hacker puede utilizar la conectividad de Internet para atacar otros sitios. Este tipo de ataque protege al hacker de ser fácilmente rastreado.

Métodos de ataque

Normalmente los hackers sin objetivo específico intentarán la explotación de un solo sistema a la vez; ataques más sofisticados pueden consistir en scripts que les permitan explotar varios sistemas a la vez.

Uso de sistemas comprometidos

Una vez que un sistema está comprometido, los hackers pueden colocar puertas traseras (en el equipo raíz (rootkit)) en el sistema, de modo que pueden acceder a el mas tarde.

Clausurar la vulnerabilidad que permitió entrar al atacante.
Cargar una puerta trasera para permitir al atacante volver a entrar.
Establecer un rastreador de contraseñas en el sistema.

Dar publicidad al acceso.
Vandalismo sobre el sistema atacado…

2.2.6 MÉTODOS DE LOS HACKERS CON OBJETIVOS ESPECÍFICOS

Los hackers con objetivos específicos están intentando penetrar o dañar una organización en particular con un objetivo concreto

Motivados por un deseo de algo que tiene la organización (normalmente algún tipo de información o dinero), como respuesta a un agravio (muchos ataques DoS son por esta causa), contratados por alguien,…

El nivel de habilidad de los hackers con objetivo específico tiende a ser mayor que el de los hackers sin objetivo específico.

Objetivos

El objetivo del ataque es la organización, no necesariamente un solo sistema dentro de la organización.

Reconocimiento para el ataque

Reconocimiento de dirección (direccionamiento IP perimetral e interno)
Identificación del espacio de dirección en uso por la organización objetivo.

Reconocimiento de números telefónicos

Reconocimiento inalámbrico

Reconocimiento del sistema
El reconocimiento del sistema es utilizado para identificar cuáles sistemas existen, qué sistema operativo están ejecutando estos y que vulnerabilidades pueden tener.
Técnicas: barridos de ping, rastreo sigiloso, rastreo de puertos,…

Reconocimiento de negocios
El entendimiento de los negocios del objetivo es muy importante para el hacker, para comprender como el objetivo usa sus sistemas, y dónde residen las capacidades e información clave, ubicación de los objetivos probables,...

Reconocimiento físico
Los hackers con objetivos específicos hacen un amplio uso del reconocimiento físico. Explota todas las debilidades en la seguridad física.

Métodos de ataque

Con toda la información reunida acerca de la organización objetivo, el hacker elegirá la vía con mayores probabilidades de éxito y el menor riesgo de detección.
El hacker con objetivo específico está intentando permanecer en el **anonimato**.
Procurará elegir métodos que no activen las alarmas.

Métodos de ataque electrónicos

Métodos de ataque físicos

Uso de sistemas comprometidos

El hacker con objetivos específicos utilizará los sistemas comprometidos para sus propósitos y, mientras tanto, borrará sus huellas lo mejor que pueda.
Este tipo de hackers no alardea de sus conquistas, actuando de forma sigilosa para no alarmar a los administradores de los sistemas objetivo.
En algunos casos pueden utilizar sistemas intermedios para atacar otros sistemas.

En la mayoría de los casos las organizaciones objetos del ataque no serán conscientes de haber sido atacados o infectados; en otros casos observarán la contaminación bien por si mismos o porque les notifiquen que su sistema está causando algún tipo de problema en Internet y limpiarán sus sistemas, pero no sabrán el uso que se ha hecho de ellos.

2.3 SOFTWARE PARA EVITAR ATAQUES

Antivirus ***Software antivirus*** ***Antispyware***

Software que vulnera la seguridad del sistema - ¿Qué ataques? - Malware

Virus
Troyanos
Gusanos
Keylogers
Dialers
Phishing
Spam
Sniffing o análisis de tráfico
Ingeniería social
Robo de hardware
Conexión no autorizada a equipos o servidores
Conexión remota
Denegación de servicio
Inundación de peticiones SYN
Spoofing o suplantación de identidad
ARP Spoofing
DNS Spoofing
Zombie

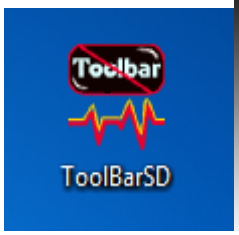
Características del programa antimalware:

Precio
Sistema operativo

Funcionalidad…eficiencia
Actualización
Instalable – portable – on-line
Valor añadido. Extras.

Ejercicio: proponer distintos programas antimalware para los sistemas operativos que utilizamos en el curso.

2.2.1 SOFTWARE RECOMENDADO



Compañías Antimalware

- Ad-Aware
- Avast!
- AVG
- Avira
- BitDefender
- ClamWin
- Dr. Web
- ESET
- Fireeye
- HijackThis
- Kaspersky
- Malwarebytes' Anti-Malware
- McAfee
- Microsoft Security Essentials
- Norman
- Norton AntiVirus
- Panda Cloud Antivirus
- Panda Security
- Sokx Pro
- Spybot - Search & Destroy
- SpywareBlaster
- Symantec
- TrustPort
- Windows Defender
- Windows Live OneCare
- Winpooch

3. SEGURIDAD DE ACCESO AL ORDENADOR

3.1 COMO PROTEGEMOS LA BIOS

Para evitar el acceso indeseado a nuestro equipo debemos asegurar el arranque del mismo mediante el uso de contraseñas.

Si analizamos el proceso de encendido del ordenador, recordaremos la importancia que tiene la BIOS en el mismo; es la encargada de localizar y cargar el sistema operativo o gestor de arranque.

Definimos la clave de supervisor para proteger el acceso a la BIOS.

Así evitamos que un intruso pueda acceder a la BIOS y modificar la secuencia de arranque del equipo.

Definición correcta de la secuencia de arranque del equipo.

Normalmente configuramos (ordenamos) la secuencia de arranque de la BIOS para que el equipo intente el arranque desde la unidad de CD/DVD, USB, RED, DISCO DURO,…
Esto conlleva un problema de seguridad si el atacante tiene acceso físico al equipo (o a la red) puesto que puede cargar su propio sistema operativo para después atacar el equipo.
Evitaremos el ataque modificando la secuencia de arranque para que el equipo solo pueda arrancar desde el disco duro.

Instrucciones para poner y quitar la contraseña de la BIOS.

3.2 COMO PROTEGEMOS EL GESTOR DE ARRANQUE

Para evitar que personas no autorizadas tengan acceso a la edición de las opciones de arranque de distintos sistemas operativos que controla el gestor de arranque, establecemos una contraseña.

Definición de contraseña en el GAG.

Definición de contraseña en el GRUB

Fichero ***/boot/grub/menu.lst***

Definición de contraseña cifrada en el GRUB

grub
md5crypt
quit

Editamos menu.lst y añadimos el password generado

Utilizar la aplicación **startupmanager** de Linux (**administración/administrador de arranque**)
Proteger con contraseña el cargador de arranque.
Comprobar que el programa startupmanager escribe las contraseñas en el fichero menu.lst

3.3 CIFRADO DE PARTICIONES

Técnica para proteger la confidencialidad de los datos almacenados en distintos volúmenes del equipo mediante el cifrado de particiones.

Bitlocker	(Windows)	
Truecrypt	(Windows/Linux)	Migración a Bitlocker para Windows
Diskcryptor	(Windows)	

Ejercicio: cifrar una partición de disco.

Estudio: proponer software alternativo.

3.4 CUOTAS DE DISCO

Mecanismos para impedir que ciertos usuarios hagan un uso indebido de la capacidad del disco, y así evitar la ralentización del equipo por saturación del sistema de ficheros y el perjuicio al resto de los usuarios al limitarles el espacio en disco.

Las cuotas de disco se pueden configurar en función de varios criterios, según usuarios, grupos o por volúmenes.

Activación y uso de cuotas de disco en Windows

(Botón derecho) sobre la partición / propiedades / cuota

Ejercicios:

Establecer cuotas para currito1 y currito2 distintas de jefe1 y jefe2.
Monitorización del estado de las cuotas de los usuarios.
Cuotas de usuario en Ubuntu
Limitar la cuota utilizando la herramienta Webmin

4. AUTENTICACIÓN DE USUARIOS

Autenticar: dar seguridad de que algo o alguien es lo que representa o parece

Los métodos de autenticación son los mecanismos que una máquina tiene para comprobar que el usuario que intenta acceder es quien dice ser.

Estos métodos se pueden clasificar en tres grupos:

Algo que el usuario sabe y que el resto de las personas desconoce.
Algo que el usuario posee.
Alguna característica propia del usuario, rasgos físicos o de comportamiento.

Hay sistemas de autenticación que combinan distintos métodos para alcanzar un mayor grado de seguridad.

Crackear contraseñas: Ejemplo

Fuerza bruta.
Diccionario
Rainbow tables.

4.1 POLÍTICA DE CONTRASEÑAS

La seguridad del sistema está fuertemente relacionada con la elección de la contraseña y la confidencialidad de la misma

En la mayoría de los equipos informáticos, la autenticación de los usuarios se realiza introduciendo un nombre y una ***contraseña***. Cada usuario tiene asignado un identificador y una clave, que permitirán comprobar la identidad del mismo en el momento de la autenticación.

Cambiar siempre la contraseña por defecto.

Las empresas suelen tener definida una **política de contraseñas** donde se establece:

Ámbito de aplicación de la política.
Longitud de la contraseña.
Formato de la contraseña.
Tiempo de vida. Limitar el tiempo de vida de la contraseña.
Forzar el historial de contraseñas; para no repetirlas.
Numero de intentos que bloquearán la cuenta. Limitar el número de intentos fallidos.
No almacenar las contraseñas copiadas en ningún sitio.
No enviar las contraseñas por correo.
No comunicar las contraseñas a nadie por teléfono.
Cambiar las contraseñas por defecto de los fabricantes.
No utilizar la misma contraseña en varias máquinas.
No permitir que las aplicaciones guarden las contraseñas.

4.2 SISTEMAS BIOMÉTRICOS

Los sistemas biométricos se utilizan para autenticar a los usuarios a través de sus rasgos físicos o conductas

¿Cómo funciona un sistema biométrico? ***Biometría***

Los tipos de sistemas biométricos más populares son:

Verificaciones anatómicas
Mano
Rostro
Patrones oculares
Verificación del comportamiento
Timbre de voz
Escritura
Longitud y cadencia del paso

Estudio: Realizar un estudio sobre dispositivos reales que implementan este tipo de autenticación.

4.3 ACL – LISTAS DE CONTROL DE ACCESO

Las listas de control de acceso (ACL) mejoran la seguridad de los archivos de nuestro sistema

ACL – Observatorio tecnológico

En dichas listas se definen los privilegios que tiene un usuario de forma individual sobre un determinado recurso, es decir, permiten o limitan el acceso a un recurso de manera individual sin tener en cuenta el grupo al que pertenece el usuario.

Listas de control de acceso en Windows XP
Listas de control de acceso en Windows 2008 Server
Listas de control de acceso en Ubuntu

Linux:

Permisos de acceso a archivos
chmod
Sistemas de ficheros, conceptos básicos
fstab
acl debian
acl gnulinux

/etc/fstab particiones donde se usan las ACL
mount – o remount,acl /dev/sda5 vuelve a montar el dispositivo después de cambiar ***fstab***

Comprobar los permisos:

ls –l

getfacl *nombredeficheroodirectorio*

Establecer permisos con ACL:

setfacl –m user:*nombreusuario****:rw-*** *nombredeficheroodirectorio*

¿Qué diferencia hay entre acl y chmod?

Windows cacls Icacls DSACLS

cacls.exe

cacls fichero /parámetros

/t	directorio actual y subdirectorio
/e	modifica la acl existente, no la remplaza
/g usuario:permisos	

Permisos utilizando el entorno gráfico.

Herencia de permisos.

5. VULNERABILIDADES DEL SISTEMA

Mantener el sistema actualizado:

Windows: **Windows Update**

Linux: **apt-get update, apt-get upgrade**

http://trucos-linux.blogspot.com.es/2010/01/diferencia-entre-apt-get-update-y-apt.html

Mantener actualizados el resto de aplicaciones y dispositivos que utilizamos.

Programas especializados en buscar actualizaciones… APPGET, UPDATE MODIFIER…

Servidor de actualizaciones para todos los equipos de la LAN.

Analizar el software descargado antes de su instalación en **www.virustotal.com**

5.1 ANALISIS DE VULNERABILIDAD

Error de software **Agujero de seguridad**

Plan de contingencias

5.2 AUDITORÍA DE SEGURIDAD

Auditoría informática

Auditoría de seguridad de sistemas de información

Ejercicio: busca en Internet ejemplos de auditorías de informáticas o auditorías de seguridad informática.

6. MONITORIZACIÓN DEL SISTEMA

log: registro de un evento que se produce en el sistema.

Con la monitorización del sistema pretendemos auditar lo eventos que se han producido o se están produciendo en nuestro equipo.

Configuración del sistema
Administración de procesos
Consolas administrativas
Administración de servicios
Monitor del sistema
Visor de sucesos
Ficheros de log

nota: **Blog**: weB LOG

6.1 WINDOWS

Monitorización W7
Monitorización Windows 2012 server

eventvwr.msc

Guarda información de los sucesos de aplicación , seguridad y sistema.

La información se guarda en los archivos **AppEvent.evt**, **SecEvent.evt** y **SysEvent.evt** ubicados en el directorio **%SystemRoot%\system32\config**.

Es muy importante configurar correctamente el tamaño y el acceso a los mismos. El tamaño debe ser lo suficientemente grande para albergar los sucesos producidos en el sistema hasta que lo auditemos. Y debemos evitar que los intrusos puedan borrar las huellas, solo deberán tener permisos de control total los encargados de la seguridad del sistema.

6.1.1 ROLES, SERVICIOS DE ROL Y CARACTERÍSTICAS

Roles, servicios de rol y características
Instalación y desinstalación de roles, servicios de rol o caracerísticas.

Ejercicio: leer y discutir los artículos anteriores; aplicarlos en un servidor W2012.

6.1.2 CONSOLAS ADMINISTRATIVAS .msc

Comandos necesarios para iniciar las distintas consolas administrativas de Windows Server 2008:

AdRmsAdmin.msc	Active Directory Rights Management Services
Adsiedit.msc	ADSI Edit
Azman.msc	Authorization Manager
Certmgr.msc	Certmgr (Certificates)
Certtmpl.msc	Certificates Template Console
CluAdmin.msc	Failover Cluster Management
Comexp.msc	Component Services
Compmgmt.msc	Computer Management
Devmgmt.msc	Device Manager
Dfsmgmt.msc	DFS Management
Dhcpmgmt.msc	DHCP Manager
Diskmgmt.msc	Disk Management
Dnsmgmt.msc	DNS Manager
Domain.msc	Active Directory Domains And Trusts
Dsa.msc	Active Directory Users And Computers
Dssite.msc	Active Directory Sites And Services
Eventvwr.msc	Event Viewer
Fsmgmt.msc	Shared Folders
Fsrm.msc	File Server Resource Manager
Fxsadmin.msc	Microsoft Fax Service Manager
Gpedit.msc	Local Group Policy Editor
Lusrmgr.msc	Local Users And Groups
Napclcfg.msc	NAP Client Configuration
Nfsmgmt.msc	Services For Network File System
Nps.msc	Network Policy Server
Ocsp.msc	Online Responder
Perfmon.msc	Reliability And Performance Monitor
Pkiview.msc	Enterprise PKI
Printmanagement.msc	Print Management
Remoteprograms.msc	TS RemoteApp Management
Rsop.msc	Resultant Set of Policy
Secpol.msc	Local Security Policy
ServerManager.msc	Server Manager
StorageMgmt.msc	Share And Storage Management
Services.msc	Services
StorExpl.msc	Storage Explorer
Tapimgmt.msc	Telephony
Taskschd.msc	Task Scheduler
Tmp.msc	Trusted Platform Module (TPM) Management
Tsadmin.msc	Terminal Services Management

Tsconfig.msc	Terminal Services Configuration
Tsgateway.msc	TS Gateway Manager
Tsmmc.msc	Remote Desktops
Uddi.msc	UDDI Services Console
Wbadmin.msc	Windows Server Backup
Wdsmgmt.msc	Windows Deployment Services
Winsmgmt.msc	WINS Manager
WmiMgmt.msc	WMI Control

6.2 LINUX

6.2.1 MONITORIZACIÓN LINUX

Comandos de monitorización

top (q para salir)
htop
finger
ps muestra los procesos cargados en memoria
ps -ef|more

pstree
uptime
who muestra los usuarios conectados
w
kill finazar la ejecución de procesos
kil -9 [PID]
xkill
df utilización del espacio de disco por los sistemas de archivos
du ***du -hs /lib***
mount montar sistemas de archivos en la estructura de directorios
fdisk gestionar la tabla de particiones
fdisk -l
last
lastb
lastlog

Entorno gráfico:

Sistema/Administración/Monitor de sistema
gnome-system-monitor paquete

Sistema/Administrador/GParted Gparted

6.2.2 LOG DEL SISTEMA – ARCHIVOS DE REGISTRO DE EVENTOS

/var/log/	Archivos de log
syslog	Información general del funcionamiento del sistema
auth-log	Control de acceso: acceso o intentos de acceso
dmesg	Mensajes del arranque del Sistema Operativo. Problemas harware
dpkg.log	Registro de instalaciones y desinstalaciones dpkg
/apt/term.log	Log del comando apt
unattended-upgrades	Registro de actualizaciones automáticas

Registro de eventos en modo gráfico:

Sistema/Administración/Visor de archivos de sucesos
gnome-utils paquete

6.2.3 ADMINISTRACIÓN REMOTA

Protocolos cliente – servidor

SSH - openSSH

Servidor

apt-get install openssh-server
service ssh status
service ssh start
finger y ***w*** para ver los usuarios conectados

/var/log/auth.log	log de conexiones
/var/log/secure	log de conexiones

Cliente

ssh -l *nombreusuario ipservidor*

Escritorio remoto en linux: VNC (Virtual Network Computing)

Servidor

apt-get install vino	servidor VNC
Sistema/Preferencias/Escritorio remoto	VNC en el entornográfico

Cliente

Aplicaciones/Internet/Visor de escritorios remotos	Cliente GNOME **vinagre**
Putty	Cliente Windows Putty
VNC	Cliente VNC para Windows
webmin	Administración remota basada en https

6.2.4 GESTIÓN DE SERVICIOS

Servicio – daemon (Disk And Execution MONitor)

/etc/ directorio donde se ubican los servicios
Parametros: ***star***, ***stop***, ***restart***, ***reload***, ***status***
/etc/init.d/ shell scripts de control
/etc/init.d/*servicio parametro*
service *servicio parametro* (Debian)
rysslog escribe en los registros del sistema
cron ejecuta las tareas programadas

Gestión de servicios en modo gráfico: BootUp-Manager

apt-get install bum paquete BootUp-Manager

Sistema/Administración/BootUp-Manager

ENLACES INTERESANTES - BIBLIOGRAFÍA

Sysinternals	**utilidades de sistema avanzadas de Microsoft**		
Malware	**Exploit**	**Hacker**	**Hackear**
Delito informático	http://www.delitosinformaticos.com/	**Hacktivismo**	
Malware	**Virus**	**www.virustotal.com**	
Hijacking	**Sniffer**	**Spoofing**	**Phishing**
Civeracoso	**Spam**	**Exploit**	
Auditoría informática		**Nmap**	**Nessus**

“Fundamentos de seguridad de redes” – Eric Maiwald – Editorial Mc Graw Hill – ISBN 970-10-4624-2

“El Tao de la monitorización de seguridad en redes – Richard Bejtlich – Editorial Pearson Educación – ISBN 84-205-4600-3

“Seguridad informática – Jose Fabián Roa Buendía – Editorial Mc Graw Hill – ISBN 978-84-481-8396-7

EJERCICIOS

1. Explica los siguientes conceptos:
   - ***Seguridad activa.***
   - ***Hacker***
   - ***Malware***
2. Enumera y explica los mecanismos de protección de acceso a un sistema informático que conozcas y utilizarías en una pequeña empresa.
3. Explica las características de los cuatro tipos de ataques: Acceso, Modificación, Denegación de Servicio y Refutación; indicando los servicios de la seguridad informática que vulneran.
4. Explica la diferencia entre los siguientes tipos de software malintencionado: Virus, Troyanos y Gusanos.
5. Explica en qué consisten los siguientes ataques y localiza algún programa o mecanismo de seguridad que pueda servir para defendernos de ellos:
   - ***Virus***
   - ***Troyanos***
   - ***Gusanos***
   - ***Keylogers***
   - ***Dialers***
   - ***Phishing***
   - ***Spam***
   - ***Sniffing o análisis de tráfico***
   - ***Exploit***
   - ***Hijacking***
   - ***Ingeniería social***
   - ***Robo de hardware***
   - ***Conexión no autorizada a equipos o servidores***
   - ***Conexión remota***
   - ***Denegación de servicio***
   - ***Inundación de peticiones SYN***
   - ***Spoofing o suplantación de identidad***
   - ***ARP Spoofing***
   - ***DNS Spoofing***
   - ***Zombie***
6. Estudio de herramientas para la ***monitorización de un sistema*** concreto y de los ***procesos*** activos. Identificación y utilidad de todos los procesos que corren en el sistema. Visor de ***eventos***. Archivos de ***Log***.

   (Windows / Linux). Ejercicio obligatorio sobre los equipos de tu empresa.

   - Gestor de software instalado en el equipo
   - Administración de procesos
   - Administración de servicios
   - Gestor de eventos
   - Administración de usuarios, grupos, unidades organizativas
   - Gestor de cuotas y administración de discos y particiones
   - Administración de dispositivos – hardware – drivers
   - Log del sistema – Registro de actividad
   - Copias de seguridad de ficheros de configuración

Avanzado

PRÁCTICAS SEGURAS

7. Password en la **BIOS** de los equipos utilizados en la empresa.
8. Configurar adecuadamente la secuencia de arranque.
9. Password (cifrado) en el **gestor de arranque** utilizado.
10. Establecer **cuotas** de uso del disco.
    - Activación y uso de cuotas de disco en w2008 aplicado en los usuarios de tu empresa.
    - Cuotas de usuario en Ubuntu. Cifrado de clave privada o simétrica
11. **Cifrado** de discos o particiones.
12. Política de **contraseñas**.
    - Definir una política de contraseñas para aplicar en la empresa.
    - Descargar la aplicación **John Dhe Ripper** (www.openwall.com) y comprobar los tiempos que tarda en descubrir contraseñas.
    - Estudia otros métodos de crackear las contraseñas de los sistemas de tu empresa.
13. **Control de acceso a los recursos**.
    - Usuarios y grupos de usuarios.
    - Listas de control de acceso: Windows / Linux
    - Recursos compartidos: Windows / Linux
    - Recursos propios de un usuario: Windows / Linux
    - Política de acceso a los recursos compartidos y propios de tu empresa.
    - Script de creación de cuentas y recursos compartidos y propios para tu empresa.
    - Script de eliminación o inhabilitación de cuentas y recursos propios para tu empresa.
14. **Antivirus** y otros programas de seguridad activa que utilices en la empresa. Elección y configuración correcta sobre los equipos de la empresa.
15. **Cortafuegos local**: ofrecer el mínimo número de puertos abiertos. Elección y configuración correcta sobre los equipos de la empresa.
16. Documentar los **servicios** necesarios y su utilidad sobre un equipo, recomendable sobre los equipos de tu empresa.
17. Configuración y seguimiento del **log de un servicio**. Recomendable sobre los servicios de tu empresa.
18. **Copia de seguridad de la configuración** de un servicio. Recomendable sobre los servicios de tu empresa.
19. Recuperación de una copia de seguridad de un servicio sobre otra máquina o sobre la misma para solucionar un problema.
20. Prueba el programa **SpoofGuard** o un programa similar que nos defiende del spoofing o phising. http://crypto.stanford.edu/SpoofGuard/
21. Estudia la posibilidad de utilizar la forma de escribir de una persona para identificarla de forma automática.

EXAMINIE SUS VULNERABILIDADES

22. Examine su información y los riesgos de su negocio u hogar. Identifique la información más importante para usted.
    - Localice la información importante y determine cómo está almacenada y protegida.
    - Determine qué tipo de ataque sería más dañino para usted. Considere lo ataques de acceso, modificación, denegación de servicio y de refutación.
    - Intente identificar como detectaría usted si cualquiera de estos ataques está a punto de presentarse.
    - Seleccione el tipo de ataque que usted sienta que sería más devastador y desarrolle una estrategia de ataque (no se limite únicamente a redes y sistemas de cómputo; incluya cualquier medio físico)

REALICE UN RECONOCIMIENTO DE UN EQUIPO CONCRETO

Monitorización del sistema, administrador de tareas, visor de sucesos.
Consolas administrativas
Ficheros de log de los servicios activos

Rastreador de puertos:	**nmap**	www.insecure.org
Escaneo de vulnerabilidades:	**nessus**	www.nessus.org

23. **Consola administrativa**. Configuración, seguimiento y mantenimiento del **log** de un servicio. Procedimiento de **inicio, parada y comprobación del estado de un servicio**. Ficheros de configuración. Copia de seguridad de la configuración. Recuperación de una copia. (Realizar este estudio con los servicios implantados en la empresa del examen práctico)

24. Utilizar **nmap** para realizar un barrido ping o un rastreo sigiloso del espacio de dirección que utilizamos.

Tenga en cuenta si los sistemas se encuentran protegidos por un cortafuegos o no.

25. Utilizar **nessus** para realizar rastreos de vulnerabilidades de los equipos identificados.

Antes de realizar este ejercicio, hablar con el administrador de red (profesor) para no provocar ningún incidente de seguridad.