

Cuando se habla de seguridad en el ámbito de las TIC a menudo se confunden los conceptos de seguridad de la información y seguridad informática. Y siendo ambos realmente importantes y similares, hay diferencias entre ellos.

En este artículo hablaremos sobre los conceptos de seguridad de la información y seguridad informática y explicaremos los pilares sobre los que se basa la seguridad de la información.

También repasaremos los elementos vulnerables de un sistema informático, el concepto de amenaza, fuentes de amenazas y tipos, así como las políticas de seguridad que adoptan las organizaciones para asegurar sus sistemas o minimizar el impacto que éstas pudieran ocasionar.

Por último utilizaremos una herramienta clásica dentro de la detección de vulnerabilidades, como es Nessus.

Seguridad de la información / Seguridad informática

Existen muchas definiciones del término seguridad. Simplificando, y en general, podemos definir la seguridad como: "Característica que indica que un sistema esta libre de todo peligro, daño o riesgo." (Villalón)

Cuando hablamos de seguridad de la información estamos indicando que dicha información tiene una relevancia especial en un contexto determinado y que, por tanto, hay que proteger.

La Seguridad de la Información se puede definir como conjunto de medidas técnicas, organizativas y legales que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad de su sistema de información.

Hasta la aparición y difusión del uso de los sistemas informáticos, toda la información de interés de una organización se guardaba en papel y se almacenaba en grandes cantidades de abultados archivadores. Datos de los clientes o proveedores de la organización, o de los empleados quedaban registrados en papel, con todos los problemas que luego acarreaba su almacenaje, transporte, acceso y procesado.

Los sistemas informáticos permiten la digitalización de todo este volumen de información reduciendo el espacio ocupado, pero, sobre todo, facilitando su análisis y procesado. Se gana en 'espacio', acceso, rapidez en el procesado de dicha información y mejoras en la presentación de dicha información.

Pero aparecen otros problemas ligados a esas facilidades. Si es mas fácil transportar la información también hay mas posibilidades de que desaparezca 'por el camino'. Si es mas fácil acceder a ella también es mas fácil modificar su contenido, etc.

Desde la aparición de los grandes sistemas aislados hasta nuestros días, en los que el trabajo en red es lo habitual, los problemas derivados de la seguridad de la información han ido también cambiando, evolucionando, pero están ahí y las soluciones han tenido que ir adaptándose a los nuevos requerimientos técnicos. Aumenta la sofisticación en el ataque y ello aumenta la complejidad de la solución, pero la esencia es la misma.

Existen también diferentes definiciones del término Seguridad Informática. De ellas nos quedamos con la definición ofrecida por el estándar para la seguridad de la información ISO/IE C 27001,
que fue aprobado y publicado en octubre de 2005 por la International Organization for Standardization (ISO) y por la comisión International Electrotechnical Commission (IEC).

“La seguridad informática consiste en la implantación de un conjunto de medidas técnicas destinadas a preservar la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio.”

Como vemos el término seguridad de la información es mas amplio ya que engloba otros aspectos relacionados con la seguridad mas allá de los puramente tecnológicos.

Seguridad de la información: modelo PDCA

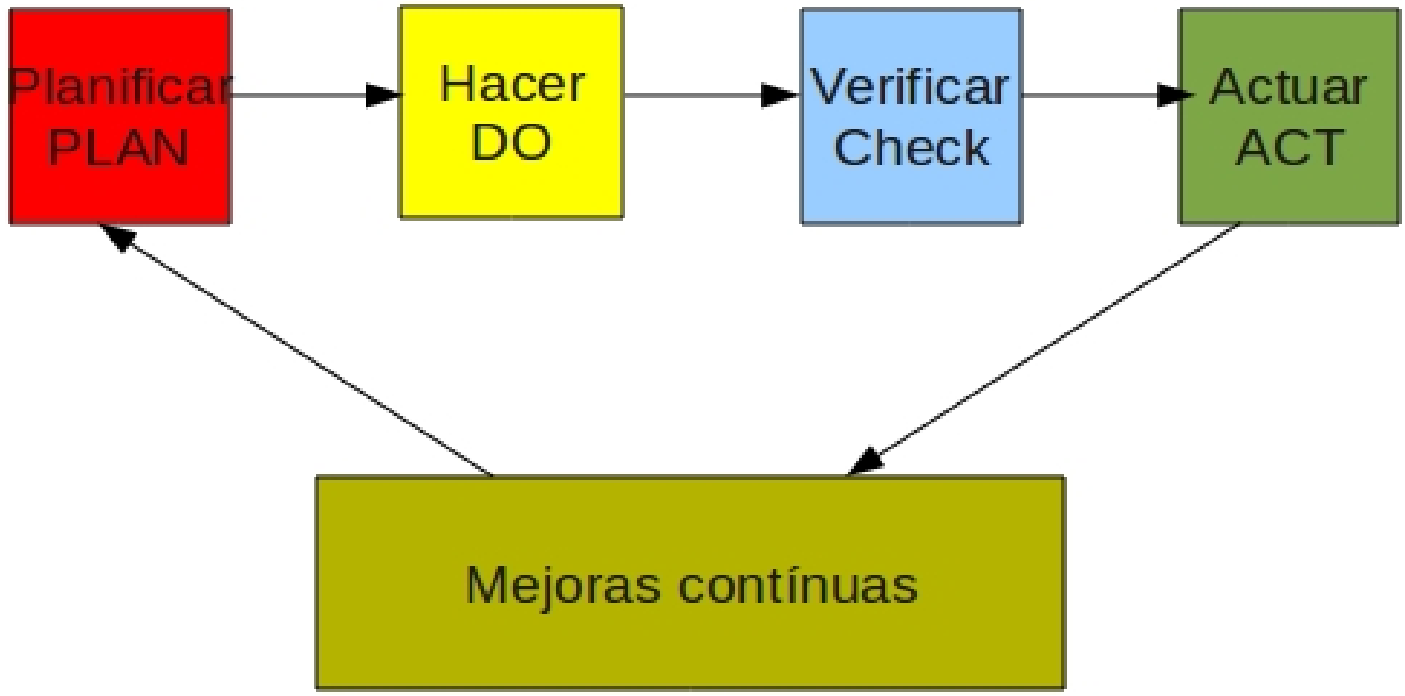
Dentro de la organización el tema de la seguridad de la información es un capítulo muy importante que requiere dedicarle tiempo y recursos. La organización debe plantearse un Sistema de Gestión de la Seguridad de la Información (SGSI).

El objetivo de un SGSI es proteger la información y para ello lo primero que debe hacer es identificar los 'activos de información' que deben ser protegidos y en qué grado.

Luego debe aplicarse el plan **PDCA** (**'PLAN – DO – CHECK – ACT**'), es decir Planificar, Hacer, Verificar, Actuar y volver a repetir el ciclo.

Se entiende la seguridad como un proceso que nunca termina ya que los riesgos nunca se eliminan, pero se pueden gestionar. De los riesgos se desprende que los problemas de seguridad no son únicamente de naturaleza tecnológica, y por ese motivo nunca se eliminan en su totalidad.

Un SGSI siempre cumple cuatro niveles repetitivos que comienzan por Planificar y terminan en Actuar, consiguiendo así mejorar la seguridad.



Bases de la Seguridad Informática

Fiabilidad

Existe una frase que se ha hecho famosa dentro del mundo de la seguridad. Eugene Spafford, profesor de ciencias informáticas en la Universidad Purdue (Indiana, EEUU) y experto en seguridad de datos, dijo que “el único sistema seguro es aquel que está apagado y desconectado, enterrado en un refugio de cemento, rodeado por gas venenoso y custodiado por guardianes bien pagados y muy bien armados. Aún así, yo no apostaría mi vida por él”.

Hablar de seguridad informática en términos absolutos es imposible y por ese motivo se habla mas bien de fiabilidad del sistema, que, en realidad es una relajación del primer término.

Definimos la Fiabilidad como la probabilidad de que un sistema se comporte tal y como se espera de él.

En general, un sistema será seguro o fiable si podemos garantizar tres aspectos:

- **Confidencialidad**: acceso a la información solo mediante autorización y de forma controlada.
- **Integridad**: modificación de la información solo mediante autorización.
- **Disponibilidad**: la información del sistema debe permanecer accesible mediante autorización.



Existe otra propiedad de los sistemas que es la Confiabilidad, entendida como nivel de calidad del servicio que se ofrece. Pero esta propiedad, que hace referencia a la disponibilidad, estaría al mismo nivel que la seguridad. En nuestro caso mantenemos la Disponibilidad como un aspecto de la seguridad.

Confidencialidad

En general el término 'confidencial' hace referencia a "Que se hace o se dice en confianza o con seguridad recíproca entre dos o más personas." (http://buscon.rae.es)

En términos de seguridad de la información, la confidencialidad hace referencia a la necesidad de ocultar o mantener secreto sobre determinada información o recursos.

El objetivo de la confidencialidad es, entonces, prevenir la divulgación no autorizada de la información.

En general, cualquier empresa pública o privada y de cualquier ámbito de actuación requiere que cierta información no sea accedida por diferentes motivos. Uno de los ejemplos mas típicos es el del ejército de un país. Además, es sabido que los logros mas importantes en materia de seguridad siempre van ligados a temas estratégicos militares.

Por otra parte, determinadas empresas a menudo desarrollan diseños que deben proteger de sus competidores. La sostenibilidad de la empresa así como su posicionamiento en el mercado pueden depender de forma directa de la implementación de estos diseños y, por ese motivo, deben protegerlos mediante mecanismos de control de acceso que aseguren la confidencialidad de esas informaciones.

Un ejemplo típico de mecanismo que garantice la confidencialidad es la Criptografía, cuyo objetivo es cifrar o encriptar los datos para que resulten incomprensibles a aquellos usuarios que no disponen de los permisos suficientes.

Pero, incluso en esta circunstancia, existe un dato sensible que hay que proteger y es la clave de encriptación. Esta clave es necesaria para que el usuario adecuado pueda descifrar la información recibida y en función del tipo de mecanismo de encriptación utilizado, la clave puede/debe viajar por la red, pudiendo ser capturada mediante herramientas diseñadas para ello. Si se produce esta situación, la confidencialidad de la operación realizada (sea bancaria, administrativa o de cualquier tipo) queda comprometida.

Integridad

En general, el término 'integridad' hace referencia a una cualidad de 'íntegro' e indica "Que no carece de ninguna de sus partes." y relativo a personas "Recta, proba, intachable.".

En términos de seguridad de la información, la integridad hace referencia a la la fidelidad de la información o recursos, y normalmente se expresa en lo referente a prevenir el cambio impropio o desautorizado.

El objetivo de la integridad es, entonces, prevenir modificaciones no autorizadas de la información.

La integridad hace referencia a:

- la integridad de los datos (el volumen de la información)
- la integridad del origen (la fuente de los datos, llamada autenticación)

Es importante hacer hincapié en la integridad del origen, ya que puede afectar a su exactitud, credibilidad y confianza que las personas ponen en la información.

A menudo ocurre que al hablar de integridad de la información no se da en estos dos aspectos.

Por ejemplo, cuando un periódico difunde una información cuya fuente no es correcta, podemos decir que se mantiene la integridad de la información ya que se difunde por medio impreso, pero sin embargo, al ser la fuente de esa información errónea no se está manteniendo la integridad del origen, ya que la fuente no es correcta.

Disponibilidad

En general, el término 'disponibilidad' hace referencia a una cualidad de 'disponible' y dicho de una cosa "Que se puede disponer libremente de ella o que está lista para usarse o utilizarse."

En términos de seguridad de la información, la disponibilidad hace referencia a que la información del sistema debe permanecer accesible a elementos autorizados.

El objetivo de la disponibilidad es, entonces, prevenir interrupciones no autorizadas/controladas de los recursos informáticos.

En términos de seguridad informática “un sistema está disponible cuando su diseño e implementación permite deliberadamente negar el acceso a datos o servicios determinados”. Es decir, un sistema es disponible si permite no estar disponible.

Y un sistema 'no disponible' es tan malo como no tener sistema. No sirve.

Como resumen de las bases de la seguridad informática que hemos comentado, podemos decir que la seguridad consiste en mantener el equilibrio adecuado entre estos tres factores. No tiene sentido conseguir la confidencialidad para un archivo si es a costa de que ni tan siquiera el usuario administrador pueda acceder a él, ya que se está negando la disponibilidad.

Dependiendo del entorno de trabajo y sus necesidades se puede dar prioridad a un aspecto de la seguridad o a otro. En ambientes militares suele ser siempre prioritaria la confidencialidad de la información frente a la disponibilidad. Aunque alguien pueda acceder a ella o incluso pueda eliminarla no podrá conocer su contenido y reponer dicha información será tan sencillo como recuperar una copia de seguridad (si las cosas se están haciendo bien).

En ambientes bancarios es prioritaria siempre la integridad de la información frente a la confidencialidad o disponibilidad. Se considera menos dañino que un usuario pueda leer el saldo de otro usuario a que pueda modificarlo.

Mecanismos básicos de seguridad

Autenticación

Definimos la Autenticación como la verificación de la identidad del usuario, generalmente cuando entra en el sistema o la red, o accede a una base de datos.

Normalmente para entrar en el sistema informático se utiliza un nombre de usuario y una

contraseña. Pero, cada vez más se están utilizando otras técnicas mas seguras.

Es posible autenticarse de tres maneras:

1. Por lo que uno sabe (una contraseña)
2. Por lo que uno tiene (una tarjeta magnética)
3. Por lo que uno es (las huellas digitales)

La utilización de más de un método a la vez aumenta las probabilidades de que la autenticación sea correcta. Pero la decisión de adoptar mas de un modo de autenticación por parte de las empresas debe estar en relación al valor de la información a proteger.

La técnica más usual (aunque no siempre bien) es la autenticación utilizando contraseñas. Este método será mejor o peor dependiendo de las características de la contraseña. En la medida que la contraseña sea más grande y compleja para ser adivinada, más difícil será burlar esta técnica.

Además, la contraseña debe ser confidencial. No puede ser conocida por nadie más que el usuario. Muchas veces sucede que los usuarios se prestan las contraseñas o las anotan en un papel pegado en el escritorio y que puede ser leído por cualquier otro usuario, comprometiendo a la empresa y al propio dueño, ya que la acción/es que se hagan con esa contraseña es/son responsabilidad del dueño.

Para que la contraseña sea difícil de adivinar debe tener un conjunto de caracteres amplio y variado (con minúsculas, mayúsculas y números). El problema es que los usuarios difícilmente recuerdan contraseñas tan elaboradas y utilizan (utilizamos) palabras previsibles (el nombre, el apellido, el nombre de usuario, el grupo musical preferido,...), que facilitan la tarea a quién quiere entrar en el sistema sin autorización.

Autorización

Definimos la Autorización como el proceso por el cual se determina qué, cómo y cuándo, un usuario autenticado puede utilizar los recursos de la organización.

El mecanismo o el grado de autorización puede variar dependiendo de qué sea lo que se está protegiendo. No toda la información de la organización es igual de crítica. Los recursos en general y los datos en particular, se organizan en niveles y cada nivel debe tener una autorización.

Dependiendo del recurso la autorización puede hacerse por medio de la firma en un formulario o mediante una contraseña, pero siempre es necesario que dicha autorización quede registrada para ser controlada posteriormente.

En el caso de los datos, la autorización debe asegurar la confidencialidad e integridad, ya sea dando o denegando el acceso en lectura, modificación, creación o borrado de los datos.

Por otra parte, solo se debe dar autorización a acceder a un recurso a aquellos usuarios que lo necesiten para hacer su trabajo, y si no se le negará. Aunque también es posible dar autorizaciones transitorias o modificarlas a medida que las necesidades del usuario varíen.

Administración

Definimos la Administración como la que establece, mantiene y elimina las autorizaciones de los usuarios del sistema, los recursos del sistema y las relaciones usuarios-recursos del sistema.

Los administradores son responsables de transformar las políticas de la organización y las autorizaciones otorgadas a un formato que pueda ser usado por el sistema.

La administración de la seguridad informática dentro de la organización es una tarea en continuo cambio y evolución ya que las tecnologías utilizadas cambian muy rápidamente y con ellas los riesgos.

Normalmente todos los sistemas operativos que se precian disponen de módulos específicos de administración de seguridad. Y también existe software externo y específico que se puede

utilizar en cada situación.

Auditoría y registro

Definimos la Auditoría como la continua vigilancia de los servicios en producción y para ello se recaba información y se analiza.

Este proceso permite a los administradores verificar que las técnicas de autenticación y autorización utilizadas se realizan según lo establecido y se cumplen los objetivos fijados por la organización.

Definimos el Registro como el mecanismo por el cual cualquier intento de violar las reglas de seguridad establecidas queda almacenado en una base de eventos para luego analizarlo.

Pero auditar y registrar no tiene sentido sino van acompañados de un estudio posterior en el que se analice la información recabada.

Monitorear la información registrada o auditar se puede realizar mediante medios manuales o automáticos, y con una periodicidad que dependerá de lo crítica que sea la información protegida y del nivel de riesgo.

Mantenimiento de la integridad

Definimos el Mantenimiento de la integridad de la información como el conjunto de procedimientos establecidos para evitar o controlar que los archivos sufran cambios no autorizados y que la información enviada desde un punto llegue al destino inalterada.

Dentro de las técnicas más utilizadas para mantener (o controlar) la integridad de los datos están: uso de antivirus, encriptación y funciones 'hash'.

Vulnerabilidades de un sistema informático

En un sistema informático lo que queremos proteger son sus activos, es decir, los recursos que forman parte del sistema y que podemos agrupar en:

-

Hardware: elementos físicos del sistema informático, tales como procesadores, electrónica y cableado de red, medios de almacenamiento (cabinas, discos, cintas, DVDs,...).

- **Software**: elementos lógicos o programas que se ejecutan sobre el hardware, tanto si es el propio sistema operativo como las aplicaciones.
- **Datos**: comprenden la información lógica que procesa el software haciendo uso del hardware. En general serán informaciones estructuradas en bases de datos o paquetes de información que viajan por la red.
- **Otros**: fungibles, personas, infraestructuras,.. aquellos que se 'usan y gastan' como puede ser la tinta y papel en las impresoras, los soportes tipo DVD o incluso cintas si las copias se hacen en ese medio, etc.

De ellos los mas críticos son los datos, el hardware y el software. Es decir, los datos que están almacenados en el hardware y que son procesados por las aplicaciones software.



Incluso de todos ellos, **el activo mas crítico son los datos**. El resto se puede reponer con facilidad y los datos ... sabemos que dependen de que la empresa tenga una buena política de copias de seguridad y sea capaz de reponerlos en el estado mas próximo al momento en que se produjo la pérdida. Esto puede suponer para la empresa, por ejemplo, la dificultad o imposibilidad de reponer dichos datos con lo que conllevaría de pérdida de tiempo y dinero.

Vulnerabilidad: definición y clasificación

Definimos Vulnerabilidad como debilidad de cualquier tipo que compromete la seguridad del sistema informático.

Las vulnerabilidades de los sistemas informáticos las podemos agrupar en función de:

Diseño

- Debilidad en el diseño de protocolos utilizados en las redes.
- Políticas de seguridad deficientes e inexistentes.

Implementación

- Errores de programación.
- Existencia de “puertas traseras” en los sistemas informáticos.
- Descuido de los fabricantes.

Uso

- Mala configuración de los sistemas informáticos.
- Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática.
- Disponibilidad de herramientas que facilitan los ataques.
- Limitación gubernamental de tecnologías de seguridad.

Vulnerabilidad del día cero

-

Se incluyen en este grupo aquellas vulnerabilidades para las cuales no existe una solución “conocida”, pero se sabe como explotarla.

Vulnerabilidades conocidas

-

Vulnerabilidad de desbordamiento de buffer.

Si un programa no controla la cantidad de datos que se copian en buffer, puede llegar un momento en que se sobrepase la capacidad del buffer y los bytes que sobran se almacenan en zonas de memoria adyacentes.

En esta situación se puede aprovechar para ejecutar código que nos de privilegios de administrador.

- Vulnerabilidad de condición de carrera (race condition).

Si varios procesos acceden al mismo tiempo a un recurso compartido puede producirse este tipo de vulnerabilidad. Es el caso típico de una variable, que cambia su estado y puede obtener de esta forma un valor no esperado.

-

Vulnerabilidad de Cross Site Scripting (XSS).

Es una vulnerabilidad de las aplicaciones web, que permite inyectar código VBSript o JavaScript en páginas web vistas por el usuario. El phishing es una aplicación de esta vulnerabilidad. En el phishing la víctima cree que está accediendo a una URL (la ve en la barra de direcciones), pero en realidad está accediendo a otro sitio diferente. Si el usuario introduce sus credenciales en este sitio se las está enviando al atacante.

-

Vulnerabilidad de denegación del servicio.

La denegación de servicio hace que un servicio o recurso no esté disponible para los usuarios. Suele provocar la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos informáticos del sistema de la víctima.

-

Vulnerabilidad de ventanas engañosas (Window Spoofing).

Las ventanas engañosas son las que dicen que eres el ganador de tal o cual cosa, lo cual es mentira y lo único que quieren es que el usuario de información. Hay otro tipo de ventanas que si las sigues obtienen datos del ordenador para luego realizar un ataque.

En http://www.cert.org/stats/ hay disponibles unas tablas que indican el nº de vulnerabilidades detectadas por año. Es interesante visitar la web de vez en cuando y comprobar el elevado número de vulnerabilidades que se van detectando. Habría que ver cuántas no se detectan...

Herramientas

En el caso de servidores Linux/Unix para hacer el análisis de vulnerabilidades se suele utilizar el programa 'Nessus'.

Nessus es de arquitectura cliente-servidor OpenSource, dispone de una base de datos de patrones de ataques para lanzar contra una máquina o conjunto de máquinas con el objetivo de localizar sus vulnerabilidades.

Existe software comercial que utiliza Nessus como motor para el análisis. Por ejemplo está

Catbird (www.catbird.com) que usa un portal para la gestión centralizada de las vulnerabilidades, analiza externamente e internamente la red teniendo en cuenta los accesos inalámbricos. Además hace monitoreo de servicios de red como el DNS y la disponibilidad de los portales web de las organizaciones.

En otros sistemas tipo Windows está el MBSA “Microsoft Baseline Security Analyzer” que permite verificar la configuración de seguridad, detectando los posibles problemas de seguridad en el sistema operativo y los diversos componentes instalados.

¿De qué queremos proteger el sistema informático?

Ya hemos hablado de los principales activos o elementos fundamentales del sistema informático que son vulnerables y ahora veremos a qué son vulnerables dichos elementos.

Comenzamos definiendo el concepto de amenaza.

Entendemos la amenaza como el escenario en el que una acción o suceso, ya sea o no deliberado, compromete la seguridad de un elemento del sistema informático.

Cuando a un sistema informático se le detecta una vulnerabilidad y existe una amenaza asociada a dicha vulnerabilidad, puede ocurrir que el suceso o evento se produzca y nuestro sistema estará en riesgo.

Si el evento se produce y el riesgo que era probable ahora es real, el sistema informático sufrirá daños que habrá que valorar cualitativa y cuantitativamente, y esto se llama 'impacto'.

Integrando estos conceptos podemos decir que “**un evento producido en el sistema informático que constituye una amenaza, asociada a una vulnerabilidad del sistema, produce un impacto sobre él** ”.

Si queremos eliminar las vulnerabilidades del sistema informático o queremos disminuir el

impacto que puedan producir sobre él, hemos de proteger el sistema mediante una serie de medidas que podemos llamar defensas o salvaguardas.

Políticas de seguridad
¿Cómo podemos proteger el sistema informático?

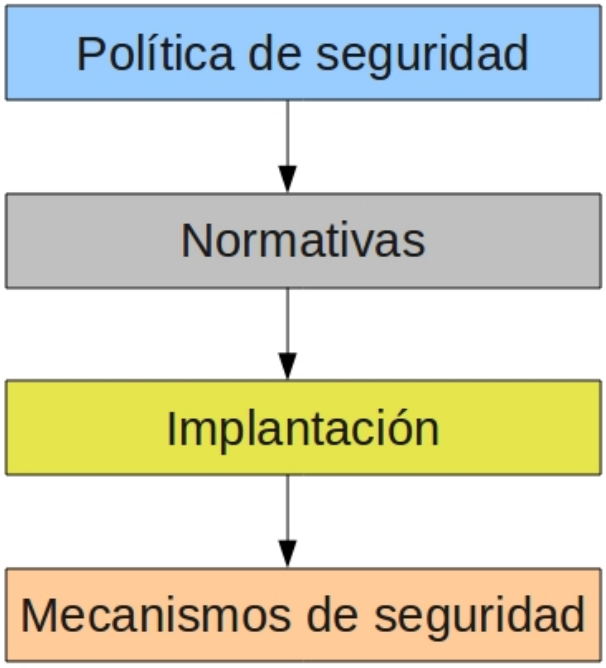
Lo primero que hemos de hacer es un análisis de las posibles amenazas que puede sufrir el sistema informático, una estimación de las pérdidas que esas amenazas podrían suponer y un estudio de las probabilidades de que ocurran.

A partir de este análisis habrá que diseñar una política de seguridad en la que se establezcan las responsabilidades y reglas a seguir para evitar esas amenazas o minimizar los efectos si se llegan a producir.

Definimos Política de seguridad como un “documento sencillo que define las directrices organizativas en materia de seguridad” (Villalón).

La política de seguridad se implementa mediante una serie de mecanismos de seguridad que constituyen las herramientas para la protección del sistema. Estos mecanismos normalmente se apoyan en normativas que cubren áreas mas específicas.

Esquemáticamente:



[redacted]su

Políticas de seguridad

El objetivo de la Política de Seguridad de Información de una organización es, por un lado, mostrar el posicionamiento de la organización con relación a la seguridad, y por otro lado servir de base para desarrollar los procedimientos concretos de seguridad.

La empresa debe disponer de un documento formalmente elaborado sobre el tema y que debe ser divulgado entre todos los empleados.

No es necesario un gran nivel de detalle, pero tampoco ha de quedar como una declaración de intenciones. Lo más importante para que estas surtan efecto es lograr la concienciación, entendimiento y compromiso de todos los involucrados.

Las políticas deben contener claramente las practicas que serán adoptadas por la compañía. Y estas políticas deben ser revisadas, y si es necesario actualizadas, periódicamente.

Las políticas deben:

- definir qué es seguridad de la información, cuales son sus objetivos principales y su importancia dentro de la organización
- mostrar el compromiso de sus altos cargos con la misma
- definir la filosofía respecto al acceso a los datos
- establecer responsabilidades inherentes al tema
- establecer la base para poder diseñar normas y procedimientos referidos a

- Organización de la seguridad
- Clasificación y control de los datos
- Seguridad de las personas
- Seguridad física y ambiental
- Plan de contingencia
- Prevención y detección de virus
- Administración de los computadores

A partir de las políticas se podrá comenzar a desarrollar, primero las normas, y luego los procedimientos de seguridad que serán la guía para la realización de las actividades.

La política de seguridad comprende todas las reglas de seguridad que sigue una organización (en el sentido general de la palabra). Por lo tanto, la administración de la organización en cuestión debe encargarse de definirla, ya que afecta a todos los usuarios del sistema.

La seguridad informática de una compañía depende de que los empleados (usuarios) aprendan las reglas a través de sesiones de capacitación y de concienciación.

Sin embargo, la seguridad debe ir más allá del conocimiento de los empleados y cubrir las siguientes áreas:

- Un mecanismo de seguridad física y lógica que se adapte a las necesidades de la compañía y al uso de los empleados
- Un procedimiento para administrar las actualizaciones
- Una estrategia de realización de copias de seguridad planificada adecuadamente

- Un plan de recuperación luego de un incidente
- Un sistema documentado actualizado

Por lo tanto y como resumen, la política de seguridad es el documento de referencia que define los objetivos de seguridad y las medidas que deben implementarse para tener la certeza de alcanzar estos objetivos.

Amenazas

Clasificación de las amenazas

De forma general podemos agrupar las amenazas en:

-

Amenazas físicas

- **Amenazas lógicas**

Estas amenazas, tanto físicas como lógicas, son materializadas básicamente por:

-

las personas

- programas específicos
- catástrofes naturales

Podemos tener otros criterios de agrupación de las amenazas, como son:

Origen de las amenazas

-

Amenazas naturales: inundación, incendio, tormenta, fallo eléctrico, explosión, etc...

- Amenazas de agentes externos: virus informáticos, ataques de una organización criminal, sabotajes terroristas, disturbios y conflictos sociales, intrusos en la red, robos, estafas, etc...
- Amenazas de agentes internos: empleados descuidados con una formación inadecuada o descontentos, errores en la utilización de las herramientas y recursos del sistema, etc...

Intencionalidad de las amenazas

-

Accidentes: averías del hardware y fallos del software, incendio, inundación, etc...

- Errores: errores de utilización, de explotación, de ejecución de procedimientos, etc...
- Actuaciones malintencionadas: robos, fraudes, sabotajes, intentos de intrusión, etc...

Naturaleza de las amenazas

La agrupación de las amenazas atendiendo al factor de seguridad que comprometen es la siguiente:

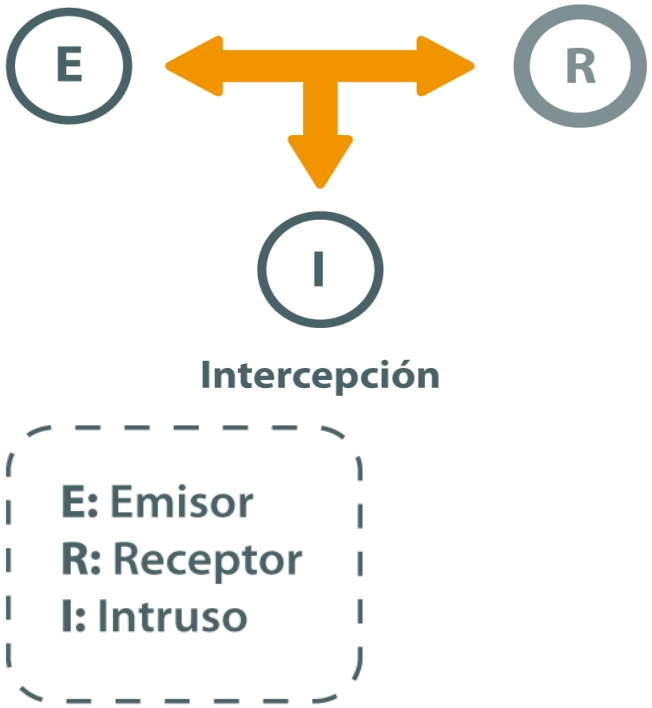
- Interceptación
- Modificación
- Interrupción
- Fabricación

1. **Flujo normal de la información**: se corresponde con el esquema superior de la figura.

Se garantiza:

- Confidencialidad: nadie no autorizado accede a la información.
- Integridad: los datos enviados no se modifican en el camino.
- Disponibilidad: la recepción y acceso es correcto.

2. **Interceptación**: acceso a la información por parte de personas no autorizadas. Uso de privilegios no adquiridos.



- Detección difícil, no deja huellas.

Se garantiza:

- Integridad.

- Disponibilidad

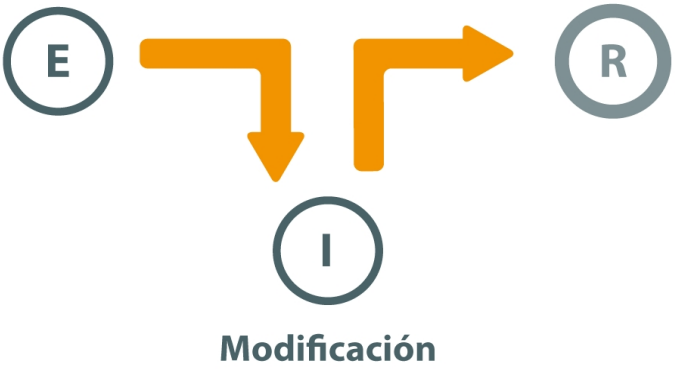
No se garantiza:

- Confidencialidad: es posible que alguien no autorizado acceda a la información

Ejemplos:

- Copias ilícitas de programas
- Escucha en línea de datos

3. **Modificación**: acceso no autorizado que cambia el entorno para su beneficio.



- Detección difícil según circunstancias.

Se garantiza:

- Disponibilidad: la recepción es correcta.

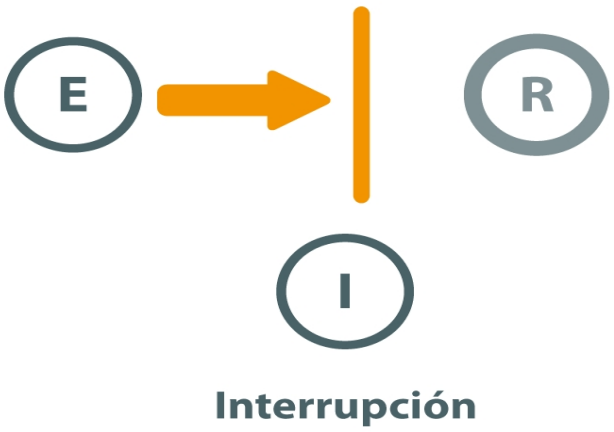
No se garantiza:

- Integridad: los datos enviados pueden ser modificados en el camino.
- Confidencialidad: alguien no autorizado accede a la información.

Ejemplos:

- Modificación de bases de datos
- Modificación de elementos del HW

4. **Interrupción**: puede provocar que un objeto del sistema se pierda, quede no utilizable o no disponible.



- Detección inmediata.

Se garantiza:

-

Confidencialidad: nadie no autorizado accede a la información.

-

Integridad: los datos enviados no se modifican en el camino.

No se garantiza:

-

Disponibilidad: puede que la recepción no sea correcta.

Ejemplos:

-

Destrucción del hardware

-

Borrado de programas, datos

-

Fallos en el sistema operativo

5. **Fabricación**: puede considerarse como un caso concreto de modificación ya que se consigue un objeto similar al atacado de forma que no resulte sencillo distinguir entre objeto original y el fabricado.



Ej[illegible] la información.

Amenazas provocadas por personas

La mayor parte de los ataques a los sistemas informáticos son provocados, intencionadamente o no, por las personas.

¿Qué se busca?

En general lo que se busca es conseguir un nivel de privilegio en el sistema que les permita realizar acciones sobre el sistema no autorizadas.

Podemos clasificar las personas 'atacantes' en dos grupos:

1. **Activos**: su objetivo es hacer daño de alguna forma. Eliminar información, modificar o sustraerla para su provecho.
2. **Pasivos**: su objetivo es curiosear en el sistema.

Repasamos ahora todos los tipos de personas que pueden constituir una amenaza para el sistema informático sin entrar en detalles:

1. Personal de la propia organización
2. Ex-empleados
3. Curiosos
4. Crackers

5. Terroristas
6. Intrusos remunerados

Amenazas físicas

Dentro de las amenazas físicas podemos englobar cualquier error o daño en el hardware que se puede presentar en cualquier momento. Por ejemplo, daños en discos duros, en los procesadores, errores de funcionamiento de la memoria, etc. Todos ellos hacen que la información o no esté accesible o no sea fiable.

Otro tipo de amenazas físicas son las catástrofes naturales. Por ejemplo hay zonas geográficas del planeta en las que las probabilidades de sufrir terremotos, huracanes, inundaciones, etc, son mucho mas elevadas.

En estos casos en los que es la propia Naturaleza la que ha provocado el desastre de seguridad, no por ello hay que descuidarlo e intentar prever al máximo este tipo de situaciones.

Hay otro tipo de catástrofes que se conocen como de riesgo poco probable. Dentro de este grupo tenemos los taques nucleares, impactos de meteoritos, etc. y que, aunque se sabe que están ahí, las probabilidades de que se desencadenen son muy bajas y en principio no se toman medidas contra ellos.

Ya hemos explicado el concepto de amenaza física. Vamos a conocer ahora cuáles son las principales amenazas físicas de un sistema informático.

Tipos de amenazas físicas

Las amenazas físicas las podemos agrupar en las producidas por:

1. Acceso físico

Hay que tener en cuenta que cuando existe acceso físico a un recurso ya no existe seguridad sobre él. Supone entonces un gran riesgo y probablemente con un impacto muy alto.

A menudo se descuida este tipo de seguridad.

El ejemplo típico de este tipo es el de una organización que dispone de tomas de red que no están controladas, son libres.

2. Radiaciones electromagnéticas

Sabemos que cualquier aparato eléctrico emite radiaciones y que dichas radiaciones se pueden capturar y reproducir, si se dispone del equipamiento adecuado. Por ejemplo, un posible atacante podría 'escuchar' los datos que circulan por el cable telefónico.

Es un problema que hoy día con las redes wifi desprotegidas, por ejemplo, vuelve a estar vigente.

3. Desastres naturales

Respecto a terremotos el riesgo es reducido en nuestro entorno, ya que España no es una zona sísmica muy activa. Pero son fenómenos naturales que si se produjeran tendrían un gran impacto y no solo en términos de sistemas informáticos, sino en general para la sociedad.

Siempre hay que tener en cuenta las características de cada zona en particular. Las posibilidades de que ocurra una inundación son las mismas en todas las regiones de España. Hay que conocer bien el entorno en el que están físicamente los sistemas informáticos.

4. Desastres del entorno

Dentro de este grupo estarían incluidos sucesos que, sin llegar a ser desastres naturales, pueden tener un impacto igual de importante si no se disponen de las medidas de salvaguarda listas y operativas.

Puede ocurrir un incendio o un apagón y no tener bien definidas las medidas a tomar en estas situaciones o simplemente no tener operativo el SAI que debería responder de forma inmediata al corte de suministro eléctrico.

Descripcion de algunas amenazas físicas

Veamos algunas amenazas físicas a las que se puede ver sometido un CPD y alguna sugerencia para evitar este tipo de riesgo.

- **Por acciones naturales:** incendio, inundación, condiciones climatológicas, señales de radar, instalaciones eléctricas, ergometría , …
- **Por acciones hostiles:** robo, fraude, sabotaje,...
- **Por control de accesos:** utilización de guardias, utilización de detectores de metales, utilización de sistemas biométricos, seguridad con animales, protección electrónica,...

Como se puede comprobar, evaluar y controlar permanentemente la seguridad física del edificio que alberga el CPD es la base para comenzar a integrar la seguridad como una función primordial dentro de cualquier organismo.

Tener controlado el ambiente y acceso físico permite:

- disminuir siniestros
- trabajar mejor manteniendo la sensación de seguridad
- descartar falsas hipótesis si se produjeran incidentes
- tener los medios para luchar contra accidentes

Las distintas alternativas enumeradas son suficientes para conocer en todo momento el estado del medio en el que se trabaja y así tomar decisiones en base a la información ofrecida por los

medios de control adecuados.

Estas decisiones pueden variar desde el conocimiento de la áreas que recorren ciertas personas hasta la extremo de evacuar el edificio en caso de accidentes.

Amenazas lógicas

El punto más débil de un sistema informático son las personas relacionadas en mayor o menor medida con él. Puede ser inexperiencia o falta de preparación, o sin llegar a ataques intencionados propiamente, simplemente sucesos accidentales. Pero que, en cualquier caso, hay que prevenir.

Entre algunos de los ataques potenciales que pueden ser causados por estas personas, encontramos:

- **Ingeniería social:** consiste en la manipulación de las personas para que voluntariamente realicen actos que normalmente no harían.
- **Shoulder Surfing:** consiste en "espiar" físicamente a los usuarios para obtener generalmente claves de acceso al sistema.
- **Masquerading:** consiste en suplantar la identidad de cierto usuario autorizado de un sistema informático o su entorno.
- **Basureo:** consiste en obtener información dejada en o alrededor de un sistema informático tras la ejecución de un trabajo.
- **Actos delictivos:** son actos tipificados claramente como delitos por las leyes, como el chantaje, el soborno o la amenaza.
- **Atacante interno:** la mayor amenaza procede de personas que han trabajado o trabajan con los sistemas. Estos posibles atacantes internos deben disponer de los privilegio mínimos, conocimiento parcial, rotación de funciones y separación de funciones, etc.

- **Atacante externo:** suplanta la identidad de un usuario legítimo. Si un atacante externo consigue penetrar en el sistema, ha recorrido el 80% del camino hasta conseguir un control total de un recurso.

Algunas amenazas lógicas

Las amenazas lógicas comprenden una serie de programas que pueden dañar el sistema informático. Y estos programas han sido creados:

- de forma intencionada para hacer daño: software malicioso o **malware** (**mal**icious soft **ware**)

- por error: bugs o agujeros.

Enumeramos algunas de las amenazas con las que nos podemos encontrar:

1. Software incorrecto

Son errores de programación (bugs) y los programas utilizados para aprovechar uno de estos fallos y atacar al sistema son los exploits. Es la amenaza más habitual, ya que es muy sencillo conseguir un exploit y utilizarlo sin tener grandes conocimientos.

2. Exploits

Son los programas que aprovechan una vulnerabilidad del sistema. Son específicos de cada sistema operativo, de la configuración del sistema y del tipo de red en la que se encuentren. Pueden haber exploits diferentes en función del tipo de vulnerabilidad.

3. Herramientas de seguridad

Puede ser utilizada para detectar y solucionar fallos en el sistema o un intruso puede utilizarlas para detectar esos mismos fallos y aprovechar para atacar el sistema. Herramientas como Nessus o Satan pueden ser útiles pero también peligrosas si son utilizadas por crackers buscando información sobre las vulnerabilidades de un host o de una red completa.

4. Puertas traseras

Durante el desarrollo de aplicaciones los programadores pueden incluir 'atajos' en los sistemas de autenticación de la aplicación. Estos atajos se llaman puertas traseras, y con ellos se consigue mayor velocidad a la hora de detectar y depurar fallos. Si estas puertas traseras, una vez la aplicación ha sido finalizada, no se destruyen, se está dejando abierta una puerta de entrada rápida.

5. Bombas lógicas

Son partes de código que no se ejecutan hasta que se cumple una condición. Al activarse, la función que realizan no esta relacionada con el programa, su objetivo es es completamente diferente.

6. Virus

Secuencia de código que se incluye en un archivo ejecutable (llamado huésped), y cuando el archivo se ejecuta, el virus también se ejecuta, propagándose a otros programas.

7. Gusanos

Programa capaz de ejecutarse y propagarse por sí mismo a través de redes, y puede llevar virus o aprovechar bugs de los sistemas a los que conecta para dañarlos.

8. Caballos de Troya

Los caballos de Troya son instrucciones incluidas en un programa que simulan realizar tareas que se esperan de ellas, pero en realidad ejecutan funciones con el objetivo de ocultar la presencia de un atacante o para asegurarse la entrada en caso de ser descubierto.

9. Spyware

Programas espía que recopilan información sobre una persona o una organización sin su conocimiento. Esta información luego puede ser cedida o vendida a empresas publicitarias. Pueden recopilar información del teclado de la víctima pudiendo así conocer contraseña o nº de cuentas bancarias o pines.

10. Adware

Programas que abren ventanas emergentes mostrando publicidad de productos y servicios. Se suele utilizar para subvencionar la aplicación y que el usuario pueda bajarla gratis u obtener un descuento. Normalmente el usuario es consciente de ello y da su permiso.

11. Spoofing

Técnicas de suplantación de identidad con fines dudosos.

12. Phishing

Intenta conseguir información confidencial de forma fraudulenta (conseguir contraseñas o pines bancarios) haciendo una suplantación de identidad. Para ello el estafador se hace pasar por una persona o empresa de la confianza del usuario mediante un correo electrónico oficial o mensajería instantánea, y de esta forma conseguir la información.

13. Spam

Recepción de mensajes no solicitados. Se suele utilizar esta técnica en los correos electrónicos, mensajería instantánea y mensajes a móviles.

14. Programas conejo o bacterias

Programas que no hacen nada, solo se reproducen rápidamente hasta que el número de copias acaba con los recursos del sistema (memoria, procesador, disco, etc.).

15. Técnicas salami

Robo automatizado de pequeñas cantidades dinero de una gran cantidad origen. Es muy difícil su detección y se suelen utilizar para atacar en sistemas bancarios.

Uso básico de Nessus

Vamos a utilizar la herramienta Nessus, desde Ubuntu, para realizar un análisis de vulnerabilidades en los equipos, por ejemplo, de la red de un aula, de la misma forma que se realizaría en una auditoría de seguridad en red.

Nessus se instala en un servidor y puede gestionarse desde una consola web remota. Existen versiones para GNU/Linux, Mac OS X, Solaris, FreeBSD y para Windows.

Instalación de Nessus

Para ello ir a http://www.tenable.com/products/nessus/nessus-download-agreement y descargar la versión de Nessus para Ubuntu 10.10 de 32 bits.

Instalar la herramienta.

Hay que ir también a la página http://www.tenable.com/products/nessus/nessus-plugins/obtain-an-activation-code , a la opción de *HomeFeed* para particulares que es gratuita. Dar los datos de nombre y correo electrónico y se recibirá el código de activación que habrá que guardar hasta que se pida.

Una vez instalado creamos un usuario para poder usarlo. Para ello ejecutamos en una terminal la orden:

```
$ sudo /opt/nessus/sbin/nessus-adduser
```

Asignar login (usuario) y contraseña y aceptar (Y). El usuario no tiene porque existir en el sistema.

Establecer este usuario como *admin* y no asignar reglas.

A continuación hay que registrarlo y es cuando se utiliza el código que se ha recibido por correo electrónico (donde XXXX-XXXX-XXXX-XXXX-XXXX es el código):

```
$ cd /opt/nessus/bin/
$ sudo ./nessus-fetch --register XXXX-XXXX-XXXX-XXXX-XXXX
Your      activation code has been registered properly - thank you.
Now       fetching the newest plugin set from plugins.nessus.org...
Your      Nessus installation is now up-to-date.
If        auto_update is set to 'yes' in nessusd.conf, Nessus will
update       the plugins by itself.
```

Indica que todo ha ido bien y comienza la actualización, si es necesaria.

Si el archivo de configuración /opt/nessus/etc/nessus/nessusd.conf indica que la actualización es automática, Nessus la hará en su momento, probablemente cuando accedamos al servicio por primera vez. En este archivo se pueden configurar otras opciones de funcionamiento de la herramienta.

También se puede hacer directamente por línea de orden:

```
$ cd /opt/nessus/sbin
$ sudo ./nessus-update-plugins
[sudo] password for elvira:
Fetching the newest updates from nessus.org...
Done. The Nessus server will restart when its scans are finished
```

No hay que cancelarla hasta que termine (puede tardar unos minutos en función del volumen de plugins a actualizar y del tipo de conexión) y muestra por terminal:

```
Your nessus instalation is up-to-date.
```

Ejecución del servicio

Ejecutar el servicio:

```
$ sudo /etc/init.d/nessusd start
```

Para comprobar que Nessus se está ejecutando correctamente ejecutar la orden:

```
$ netstat -atunp | grep nessusd
```

El puerto de escucha de Nessus es el 1241. Para el entorno gráfico el puerto utilizado es el 8834.

Utilización en modo consola

Hay que cerrar la consola gráfica.

```
$ cd /opt/nessus/sbin
$ sudo ./nessus-service -D
$ nessusd (Nessus) 4.4.1 [build M15078] for Linux
(C) 1998 - 2011 Tenable Network Security, Inc.
Processing the Nessus plugins...
[##################################################]
All plugins loaded
$ sudo vi /opt/nessus/bin/targets.txt
```

Hay que crear el archivo **targets.txt** donde se encuentran los hosts a escanear. El archivo debe contener el host o la IP.

```
$ sudo ./nessus -q 127.0.0.1 1241 usuario_nessus contraseña_usuario /opt/ne
```

El archivo targets debe ser creado antes de ejecutar el cliente, con un nombre cualquiera y guardado donde se quiera ,pero especificando la ubicación. En el archivo **res ultados.txt**
van los logs del escaneo.

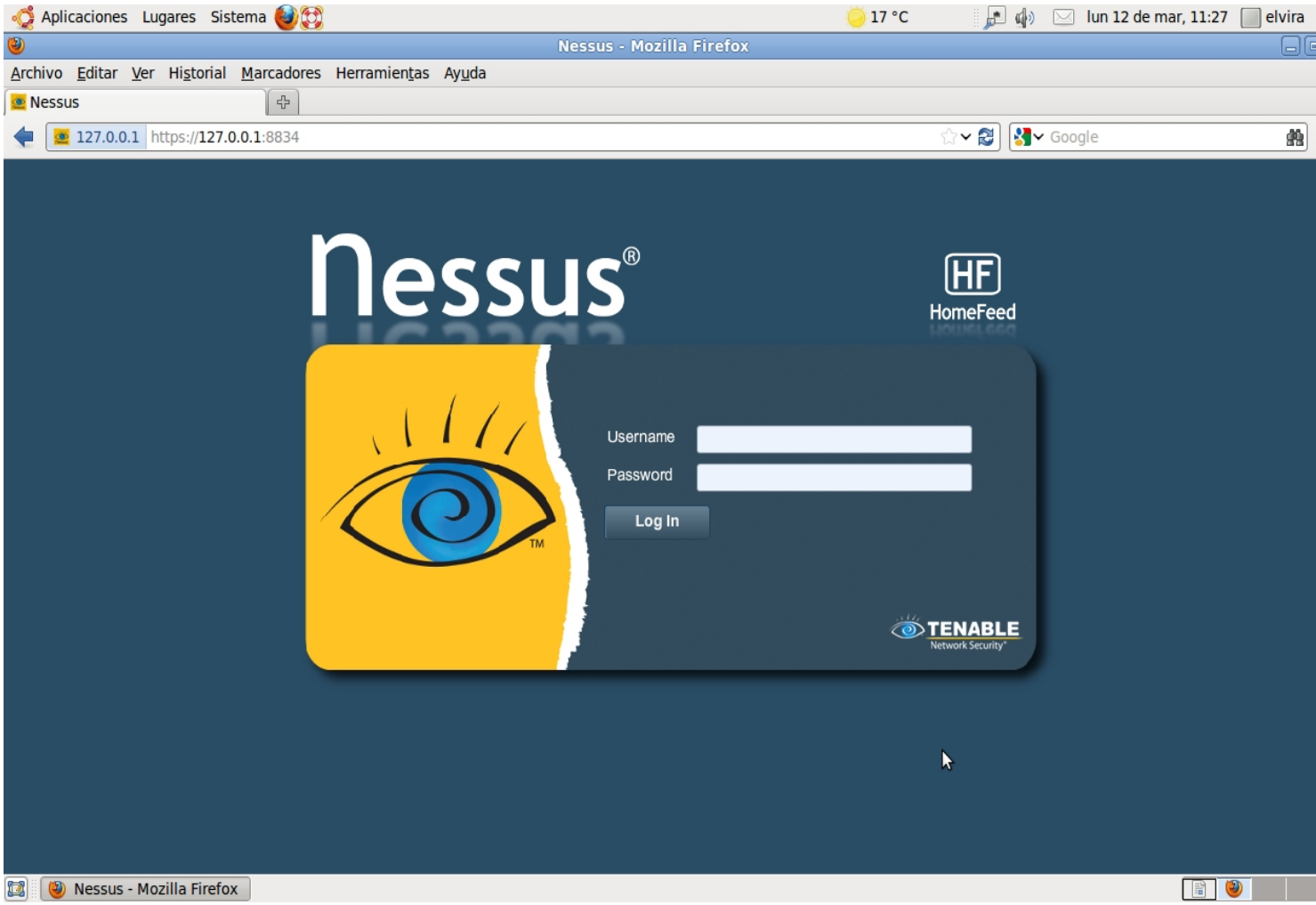
Utilización desde el navegador web

Para ello hay que abrir una nueva pestaña en el navegador para acceder a la consola web de administración y teclear en URL:

https://localhost:8834 / https://ip_servidor:8834

Aceptar la advertencia de seguridad del certificado digital y aparecerá la ventana de login, en la que introducimos el login y contraseña del usuario que se creó.

La imagen siguiente muestra lo que hemos de ver en el navegador:



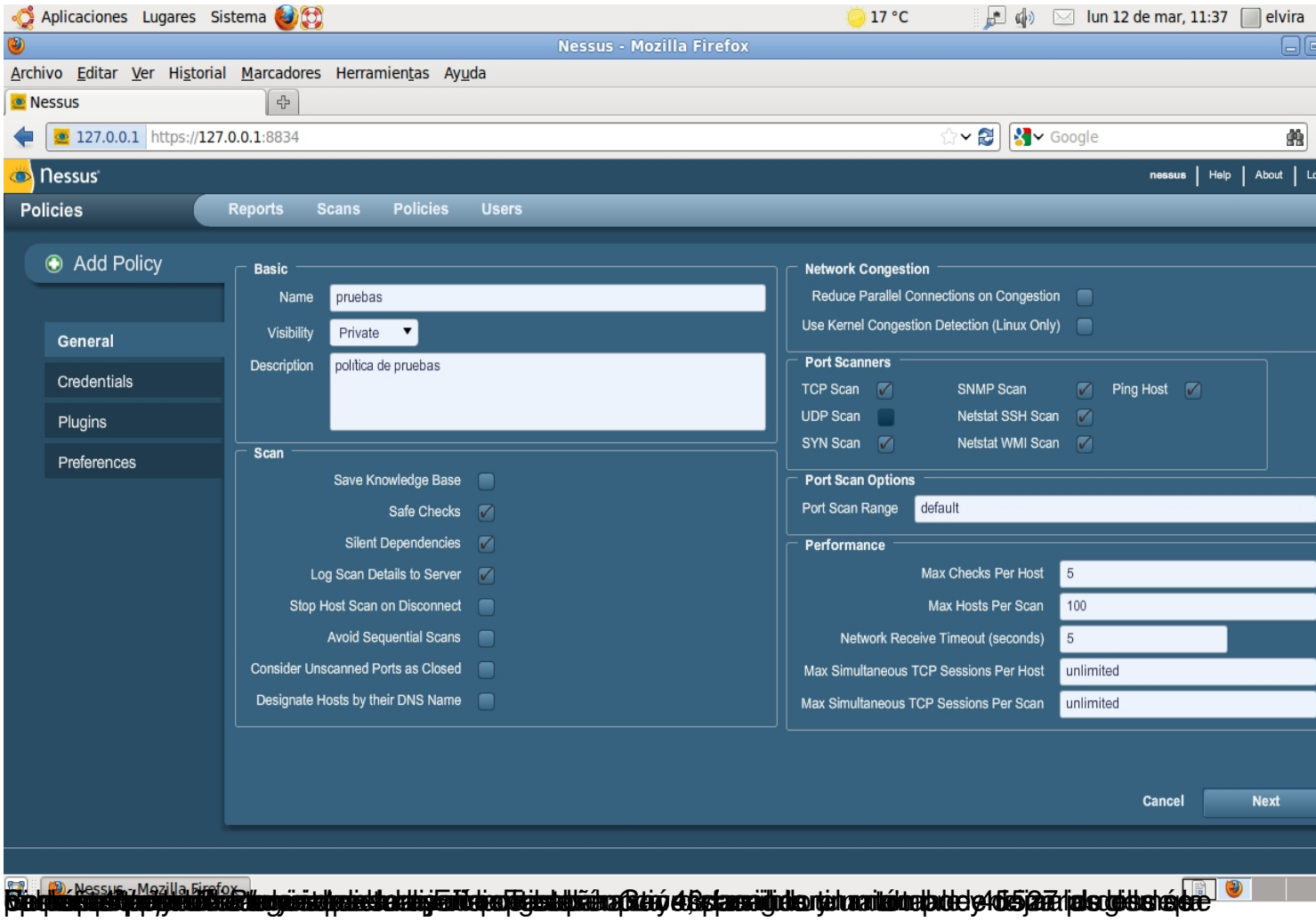
Políticas de uso

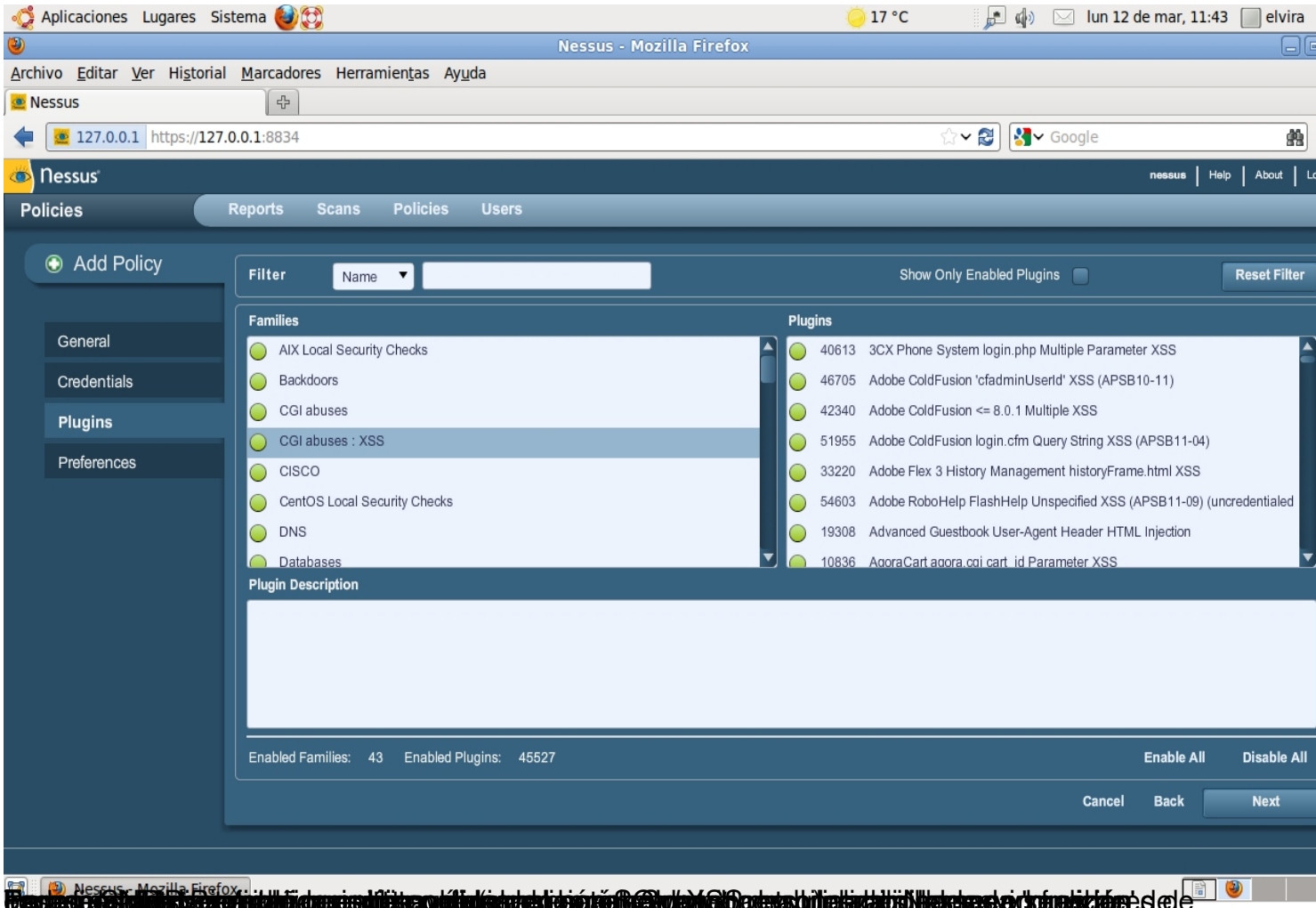
Para realizar un escaneo de vulnerabilidades es necesario crear una política.

Definir una política consiste en establecer un conjunto de opciones de configuración para ejecutar el escaneo de vulnerabilidades. Incluye parámetros como:

- sesiones TCP por host, número de hosts objetivo, tipo de escaneo,...
- credenciales para escaneos (Windows, SSH), escaneos autenticados contra Oracle, HTTP, FTP, POP, IMAP o Kerberos

Para crear la política ir a la pestaña *Policies* y pulsamos *Add*.


Aplicaciones Lugares Sistema
17 °C
lun 12 de mar, 11:37
elvira
Nessus - Mozilla Firefox
Archivo Editar Ver Historial Marcadores Herramientas Ayuda
Nessus
127.0.0.1 https://127.0.0.1:8834
Google
Nessus
nessus Help About
Policies
Reports Scans Policies Users
Add Policy
General
Credentials
Plugins
Preferences
Basic
Name pruebas
Visibility Private
Description política de pruebas
Scan
Save Knowledge Base
Safe Checks
Silent Dependencies
Log Scan Details to Server
Stop Host Scan on Disconnect
Avoid Sequential Scans
Consider Unscanned Ports as Closed
Designate Hosts by their DNS Name
Network Congestion
Reduce Parallel Connections on Congestion
Use Kernel Congestion Detection (Linux Only)
Port Scanners
TCP Scan
SNMP Scan
Ping Host
UDP Scan
Netstat SSH Scan
SYN Scan
Netstat WMI Scan
Port Scan Options
Port Scan Range default
Performance
Max Checks Per Host 5
Max Hosts Per Scan 100
Network Receive Timeout (seconds) 5
Max Simultaneous TCP Sessions Per Host unlimited
Max Simultaneous TCP Sessions Per Scan unlimited
Cancel
Next
Nessus - Mozilla Firefox



Escaneo de vulnerabilidades

Ir a la pestaña *Scans > Add* y asignar un nombre.

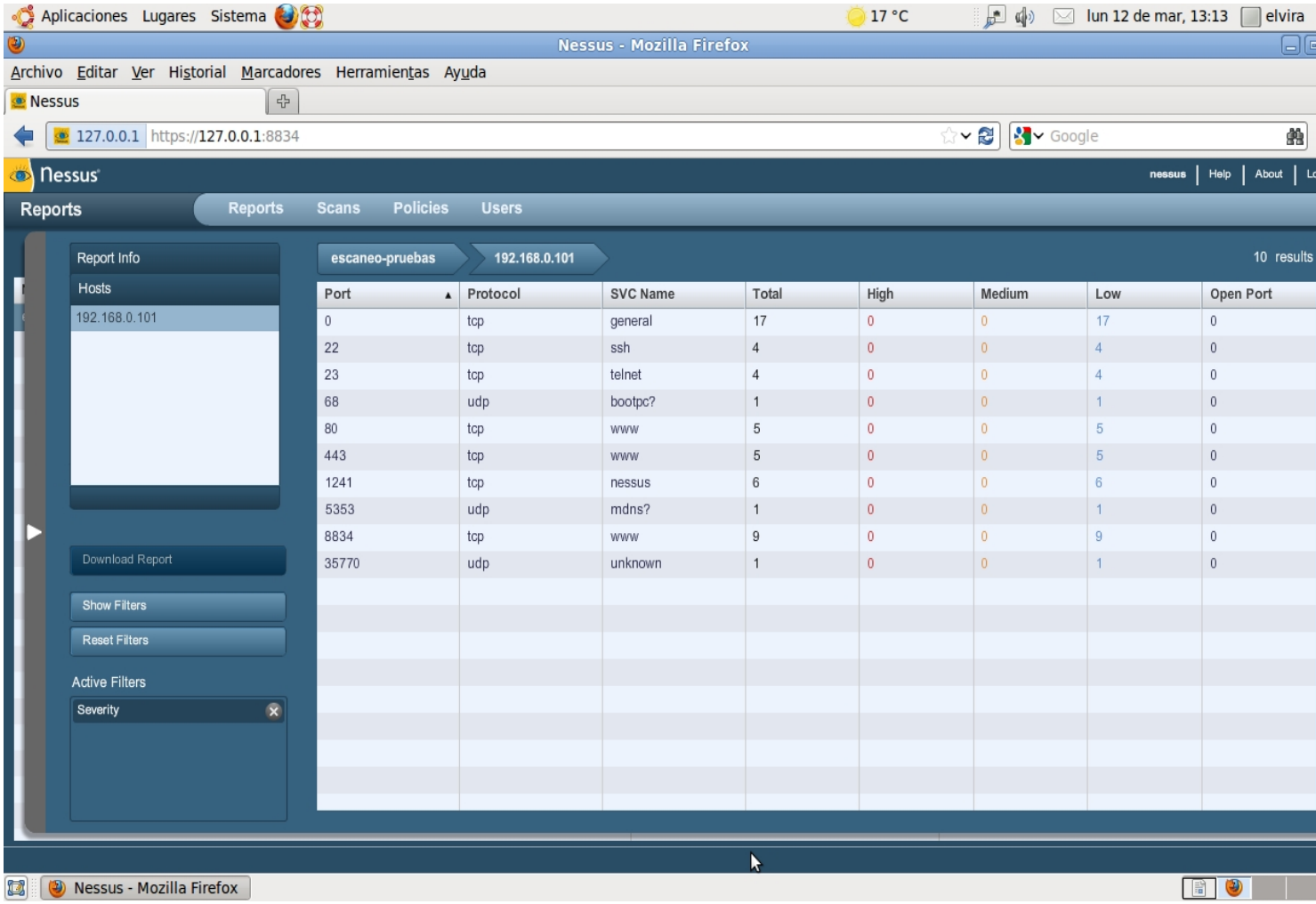
Seleccionar la política creada anteriormente 'pruebas' y escribir las direcciones IP de los hosts objetivos, indicando sus direcciones IP una en cada línea.

Ejecutar el escaneo pulsando *Launch Scan*.

Sobre la marcha desde *Browse* podemos hacer el seguimiento o desde la pestaña *Scans* o *Re ports*
se puede consultar el estado del escaneo.

Una vez ha terminado se puede consultar en la pestaña *Reports*. Haciendo clic en el informe generado, se pueden ver los equipos analizados (en nuestro caso solo una IP) así como la cantidad de vulnerabilidades o alertas y su riesgo.

Podemos ver agrupadas las vulnerabilidades en función del riesgo: bajo, medio, alto, puertos abiertos, etc.



Haciendo clic en cada una de las líneas se puede ver información relacionada con la vulnerabilidad o aviso e incluso referencias a webs donde se puede encontrar la solución.

Escaneo con credenciales de administrador

Si utilizamos el análisis con credenciales se pueden detectar muchas mas vulnerabilidades de tipo High.

Para realizar un análisis más exhaustivo, primero se debe crear una política con credenciales definidas. Para ello ir a la pestaña *Policies* y crear una nueva o copia la anterior con el botón *C opy*
.

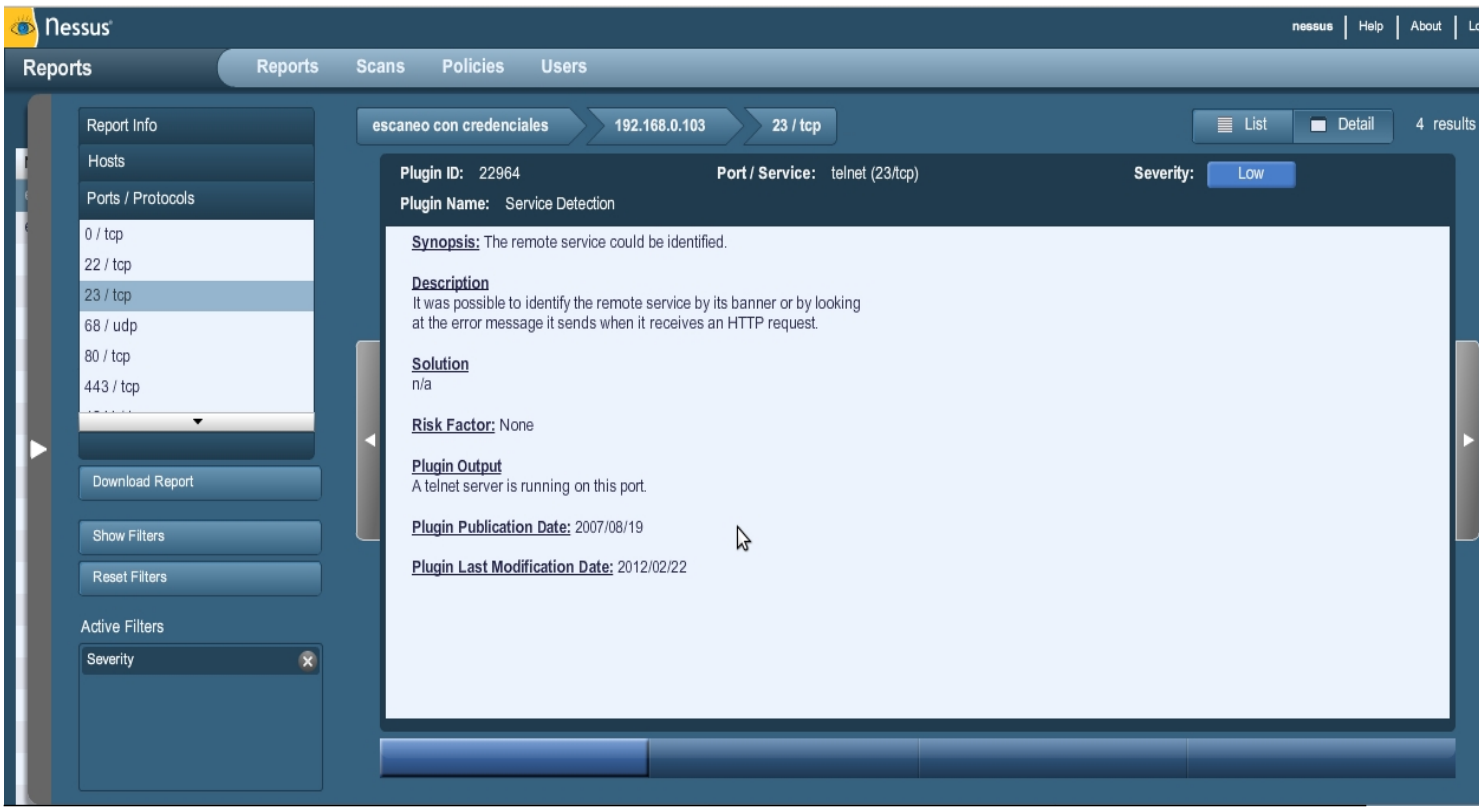
Editar la nueva política creada, asignar un nombre y desde la pestaña *Credenciales* introducir el usuario y contraseña de un usuario con suficientes privilegios tanto en Windows como en GNU/Linux.

Recordar que el usuario creado en el proceso de instalación de Ubuntu es un usuario sudo (permisos de administrador). Esta contraseña hay que definirla como tipo de credencial *SSH settings*
.

Para equipos con Windows, hay añadir la credencial como tipo *Windows credentials*. Para ello hay que asegurarse que los equipos Windows que se van a analizar tienen una contraseña definida como Administrador.

Podemos guardar la política y crear un nuevo escaneo asignándole la política con credenciales que acabamos de crear.

Para cada vulnerabilidad detectada, sea del nivel que sea, emite un informe asociado en el que da información relacionada. En la captura vemos el informe de telnet, que lo ha detectado como vulnerabilidad del sistema.



Conclusión y enlaces

En el artículo hemos hecho una introducción general a la seguridad informática, los pilares sobre los que se basa y diferentes conceptos relacionados con la seguridad, como son vulnerabilidad, amenaza, ataque, etc.

Hemos introducido también una primera herramienta relacionada con la detección de vulnerabilidades del sistema que podemos aplicar en el aula y conocer cuáles son las debilidades de nuestros sistemas para aplicar las medidas correctoras apropiadas. La herramienta es Nessus que es un clásico ya dentro de la seguridad y además disponible para diferentes plataformas.

Algunos portales importantes relacionados con seguridad, son:

-

http://www.securityfocus.com /

Es una de las bases de datos mas consultadas por los profesionales en seguridad informática por el contexto técnico aportado.

-

http://www.osvdb.org/

Esta base de datos tiene la mejor información sobre vulnerabilidades en el software open source.

-

http://secunia.com/

Secunia, tienen las mejores estadísticas de la aparición de vulnerabilidades por sistema operativo.

-

http://www.kb.cert.org/vuls/

Al igual que securityfocus, es una de las bases de datos mas consultadas por los profesionales en seguridad informática por el contexto técnico aportado.

-

http://www.zone-h.org

En su zona restringida muestra gran cantidad de información sobre ataques y estadísticas.

Utilizamos indistintamente los términos organización y empresa.

Recordar que un CPD es un Centro de proceso de datos, y en él se ubican los recursos necesarios para procesar la información de una organización.

Recordar que la "*La **Ergonomía** es una disciplina que se ocupa de estudiar la forma en que interactúa el cuerpo humano con los artefactos y elementos que lo rodean, buscando que esa interacción sea lo menos agresiva y traumática posible.*
"

Introducción a la Seguridad Informática
26/26