Seguridad en redes de ordenadores: Introducción y definiciones básicas

Escuela Tec. Superior Ingeniería de Telecomunicación

http://gsyc.urjc.es

Enero de 2015

Convenciones empleadas

En español, la conjunción disyuntiva *o* tiene dos significados opuestos

- Diferencia, separación, términos contrapuestos
  carne o pescado, blanco o negro
- Equivalencia
  alquiler o arrendamiento, *arreglar o reparar*

Para evitar esta ambigüedad, usaremos dos siglas muy comunes en inglés

- Para indicar oposición, *versus*, abreviada como *vs*
  p.e. *comprar vs alquilar*
- Para indicar equivalencia, *also known as*, abreviado *aka*
  p.e. el rey *aka* el monarca

Seguridad de una red informática

Es una definición controvertida, una definición operacional puede ser

- *Un sistema informático (hardware, software, red) es seguro si sus usuarios pueden confiar en que se comportará de la manera esperada*

Si espero acceder a mis datos, pero no puedo, esto es un fallo de seguridad. Tanto si la causa es un intruso, un fallo en el software o un incendio

- La seguridad nunca es algo absoluto. Con la suficiente (motivación/tiempo/dinero/habilidad/suerte) un atacante siempre podrá comprometer un sistema

Para ISO-7498/OSI

- Seguridad informática: mecanismos que minimizan la vulnerabilidad de bienes y recursos
- Bien: algo de valor
- Vulnerabilidad: debilidad que se puede explotar para violar un sistema o la información que contiene.

La publicidad puede afirmar que un producto es seguro porque

- El código es secreto
- El código es público
- Esa construido partiendo de cero, así que no hereda errores de código anticuado
- Está construido a partir de código usado masivamente por la industria
- No se ejecuta como root/administrator
- No funciona sobre Unix
- No funciona sobre Windows
- No se conoce ningún ataque contra él
- Emplea criptografía de clave pública

Pero nada en esta lista garatiza la seguridad

Seguridad:Soluciones técnicas

- Nivel físico: Proteger el cable de escuchas
  ¿y si no hay cable?
- Nivel de enlace: Cifrar al enviar y descifrar al recibir
- Nivel de red: IPsec, cifrado en IPv6. Cortafuegos
- Nivel de transporte: Cifrado de conexiones. SSL

Problemas:

- La mayoría de los SSOO y protocolos actuales (Unix/Linux, Windows) fueron diseñados originalmente antes de la omnipresencia de internet.
- IP no fue diseñado originalmente pensando en la seguridad
- No solo hay fallos de seguridad técnicos, sino humanos, relativos a *ingeniería social*

Tipos de seguridad

- Confidencialidad/secreto
  Solo las personas autorizadas tienen acceso a leer (y por tanto copiar) la información
- Integridad de los datos
  Tener la garantía de que el dato/programa/mensaje lo ha generado la persona adecuada y nadie lo ha alterado. Ya sea mensaje online, dato en disco, backup, papel...
  Nótese que si el mensaje se altera, pero tenemos constancia de la alteración, la integridad sigue garantizada (el mensaje se ha perdido pero no se ha alterado)
- Disponibilidad
  Los servicios deben estar disponibles de la forma prevista

¿Es posible la integridad sin confidencialidad?
¿Es posible la confidencialidad sin integridad?

- Consistencia
  El sistema debe comportarse correctamente, de la forma esperada
- Control de acceso
  Mecanismo que determina qué o quién puede interactuar con un recurso

- Control/auditoría
  Posibilidad de saber quién ha accedido a qué recurso, cuándo y cómo
- No repudio
  Mecanismo que impide que las entidades que participan en una comunicación nieguen haberlo hecho
  - No repudio con prueba de origen
  - No repudio con prueba de destino

Motivación del atacante

- Actualmente los ordenadores conectados a la red son omnipresentes: usuarios particulares, todo tipo de empresas, comercios, bancos, hospitales, organismos gubernamentales...
- Un ataque puede ser muy dañino

Diversa motivación de los atacantes

- *Diversión*, reto personal
- Vandalismo
- Robo de información buscando beneficio o chantaje
- *Activismo* político
- Crimen organizado, terrorismo
- Espionaje
- Etc

Los mayores riesgos provienen de empleados o ex-empleados

El resultado de un ataque puede ser

- Una pérdida económica directa
- Pérdida de muchos otros activos,
  - p.e. la imagen de la víctima en un *website defacement*

Simplemente *echar un vistazo* causa un daño serio y compromete un sistema

- Comprometer
  (2)Exponer o poner a riesgo a alguien o algo en una acción o caso aventurado

Hackers

- *Hack* en inglés ordinario, significa cortar en rodajas, cortar en tajos, trocear, desbrozar...
- A partir de los años 60, en informática, se le da el significado de *truco*: usar, configurar o programar un sistema para ser usado de forma distinta a la esperada habitualmente
- *Hacker* significa, entre otras cosas, una persona que se *cuela* en un ordenador o red de ordenadores. Es una palabra que no tiene una definición universalmente aceptada
  - En el lenguaje, prensa y medios generalistas, *hacker* suele tener connotacciones negativas
  - En la comunidad especializada, para una persona que comete delitos se emplea el término *cracker*

hacker n.
[originally, someone who makes furniture with an axe]

1. A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary
2. One who programs enthusiastically (even obsessively) or who enjoys programming rather than just theorizing about programming
3. A person capable of appreciating hack value
4. A person who is good at programming quickly
5. An expert at a particular program, or one who frequently does work using it or on it; as in *a Unix hacker*
6. An expert or enthusiast of any kind. One might be an astronomy hacker, for example
7. One who enjoys the intellectual challenge of creatively overcoming or circumventing limitations.
8. (deprecated) A malicious meddler who tries to discover sensitive information by poking around. Hence *password hacker*, *network hacker*. The correct term for this sense is *cracker*

Eric S. Raymond, The jargon file v4.2.0

Clasificación de los hackers

Según su motivación

- *White hat hacker*. Motivación legítima, *hacking* ético. Prueba su propio sistema o el de otro, por el que está contratado, con autorización previa explícita
  - *Red team*: Atacantes
  - *Blue team*: Defensores
- *Grey hat hacker*. Invade un sistema sin autorización del responsable, notifica posteriormente que ha podido burlar la seguridad. Tal vez solicite una cantidad de dinero *razonable*
- *Black hat hacker*. *Cracker*. Delincuente. Actividades de vandalismo, fraude, robo de identidad, piratería...

Según su nivel de conocimientos, en los extremos están

- Elite: Minoría más avanzada que es capaz de descubrir técnicas nuevas
- *Neophyte, noob, newbie*: principiante
- *Lamer*: persona que alardea de habilidades de las que carece, con falta de capacidad y de conocimiento. A pesar de tener experiencia
- *Script kiddie*: principiante que no sabe lo que hace, usa ciegamente aplicaciones desarrolladas por otros sin comprenderlas ni saber adaptarse a un mínimo cambio

Otros términos relativos a personas

- BOFH: bastard Operator From Hell (infame administrador del demonio). Personaje de los libros de S.Travaglia. Por extensión, administrador de sistemas autoritario
- Luser (loser+user). Usuario ordinario (despectivo)
- Spammer: persona que envía correo basura
- Phreaker: usuario con conocimientos avanzados sobre las redes de telefonía, que puede llegar a hacer actividades no autorizadas

Gestión del riesgo

Preguntas clave para mejorar la seguridad de nuestro sistema

- ¿Qué intento proteger y cuánto vale para mi?
- ¿Qué necesito para protegerlo?
- ¿Cuanto tiempo, esfuerzo y dinero estoy dispuesto a emplear? Es necesario el apoyo de la dirección de la empresa/organismo, en autoridad y recursos

Para ello es necesario

- Identificación de los activos (*assets*) y de su valor
- Indentificación de las amenazas
- Cálculo de los riesgos
  - Mediante análisis *coste-beneficio*
  - Mediante *best practices* (prácticas recomendables)

Indentificación de los activos

- Tangibles:
  Ordenadores, equipos de comunicaciones y cableado, datos, backups, libros, software comprado, etc
- Intangibles:
  Salud e integridad física del persona, privacidad, contraseñas, reputación, disponibilidad

No debemos limitar los activos al ámbito de la red. P.e. una contraseña es un activo, ya esté en un fichero con cifrado fuerte o en un *post it*

Identificación de los riesgos

- Malware, crackers, etc
- No disponibilidad de personal:
  Enfermedad: individual o epidemia. Bajas
- No disponibiliad de un servicio:
  Red, energía
- Inundación, fuego, sabotaje, vandalismo
- Robo de soporte de datos, ordenadores de escritorio, portátiles
- Vulneración de NDA (*Non-disclosure agreement*)
- Desaparición de proveedor de bienes o servicios
- Fallo hardware
- Fallo software
- ...

Análisis coste-beneficio

Procedimiento común en muchas ingenierías

- Calcular el coste de la pérdida de un activo
- Calcular la probabilidad de una pérdida
- Calcular el coste de la prevención

Decidir con todo ello las medidas a tomar

Best practices/prácticas recomendables

- El análisis coste-beneficio puede ser de utilidad, pero en el ámbito de las TIC es de difícil aplicación
- De forma complementaria/alternativa se desarrollan una serie de normas prácticas, recomendaciones, (*rules of thumb*), relativamente universales y consensuadas por la comunidad de especialistas en seguridad: las *best practices*

Ejemplo de prácticas recomendables

- Seguridad física: todo acceso físico al equipo de red debe estar convenientemente protegido: acceso a estancias, armarios, llaves, etc
- Todas las aplicaciones, SSOO y *drivers* deben actualizarse con regularidad
- Todas las contraseñas deben ser de calidad
- El acceso remoto debe limitarse por usuario y por dirección IP
- Avisos legales en pantallas de login, constancia de que las normas han sido comunicadas y aceptadas, etc

- Contamos con el apoyo de un SOC (*Security Operations Center*)
  Es un organismo especializado en seguridad, monitoriza el malware, analiza nuevos riesgos, advierte a la comunidad de usuarios, está en contacto con otros SOC, etc
- Cierta monitorización de la actividad de los usuarios
- *Timeout* adecuado para el cierre de sesiones por inactividad

- Deshabilitación de todos los servicios no necesarios
- Tráfico inalámbrico encriptado correctamente
- Uso correcto de cortafuegos
- Uso correcto de antivirus (especialmente a la entrada de la red)
- Uso de VPN para tráfico que circule por redes públicas
- Uso de VLAN si es necesario segregar servicios y/o usuarios dentro de la organización
- Control de dirección IP/MAC por parte de los switches
- Uso de versiones seguras de los protocolos. Actualización de rutas, DNS, etc
- Mecanismos de auditoría funcionando correctamente
- Test de intrusión, preferentemente realizado por especialista externo