Ataques y contramedidas (I)

Alberto Molina Coballes

IES Gonzalo Nazareno
CONSEJERÍA DE EDUCACIÓN

15 de abril de 2012

Introducción

- Vamos a conocer la terminología básica sobre ataques y contramedidas.

Ataque informático Método mediante el cual un atacante (individuo o programa) intenta o realiza una o varias de las siguientes acciones sobre un sistema informático (equipo físico, sistema, aplicación o datos):

- Acceso no permitido
- Daño
- Desestabilización

Contramedida Mecanismos utilizados para defenderse de un ataque. Hay contramedidas preventivas (para evitar el ataque o reducir sus consecuencias) y paliativas (para reducir el daño del ataque).

Algunas definiciones más

Hacker Personas que disfrutan conociendo en profundidad sistemas y redes. Se habla de cultura hacker y fueron el origen de Internet o el movimiento de software libre.

Cracker Personas que conocen en profundidad la seguridad de los sistemas informáticos y lo utilizan para atacarlos.

Lamer o script-kiddie Ignorante que ejecuta código de otros sin saber qué hace ni con qué consecuencias. Se autodefine como hacker (y de los buenos!)

Juánker Véase la Frikipedia ;)

Black Hat Crácker

Grey Hat Crácker a tiempo parcial ...

White Hat Hacker en el sentido explicado aquí.

Ubicación del atacante

- Las posibilidades de ataque se relacionan directamente con la cercanía al equipo atacado, así se distinguen:

  Acceso físico al equipo Un atacante con acceso físico tiene muchas facilidades para acceder de forma no permitida, provocar daños en el equipo o desestabilizarlo.

  Acceso directo al equipo (sesión) Alguien que pueda abrir una sesión puede realizar un gran número de ataques, que tendrán mayor repercusión cuanto mayores sean los privilegios del usuario con el que se accede.

  Acceso a la red local del equipo Se pueden realizar diferentes acciones, fundamentalmente orientadas a poder acceder posteriormente al equipo objetivo.

  Acceso a través de Internet Más limitada que la anterior en principio, al no tener acceso al nivel de enlace en las comunicaciones con el equipo objetivo.

Potenciales atacantes

- El número de potenciales atacantes se suele relacionar de forma inversa con la ubicación de los mismos, así una situación típica podría ser:
  - Pocas personas tienen acceso físico al equipo.
  - Algunas personas tienen acceso a una sesión en el equipo.
  - Todas las personas de la organización tienen acceso a un equipo de la red local.
  - Todo Internet tiene acceso remoto al equipo.
- Un ataque desde Internet podría atacar tanto al equipo objetivo como a otro cualquiera de su red, posteriormente intentar abrir una sesión e ir ganando privilegios en el equipo objetivo.

Principales ataques con acceso físico

- Las posibilidades de provocar daños o desestabilización son obvias: destruir el equipo, robarlo, apagarlo, reiniciarlo, ...
- La seguridad física estudia principalmente lo métodos para evitar que una persona no autorizada tenga acceso a los equipos.
- Con respecto a los accesos no autorizados:
  - Obtención directa de los datos
  - Obtención de contraseñas (*password cracking*)
  - Ejecución de otro sistema operativo sobre el sistema
- Contramedidas:
  - Protección de la BIOS
  - Protección del gestor de arranque
  - Cifrado del sistema de ficheros o de ficheros concretos
  - Utilización de contraseñas fuertes

Principales ataques sobre una sesión

Malware

- Bien de forma intencionada o no, un usuario que pueda abrir una sesión puede provocar serios problemas de seguridad, ya que en su sesión puede instalarse todo tipo de malware:
  - Virus
  - Gusanos (*worm*)
  - Puertas traseras (*backdoors*)
  - *Rootkits*
  - Caballos de Troya o Troyanos (*trojan horses*)
  - *Spyware*
  - Equipo zombie. Botnet
  - *Keylogger*
  - *Dialer*

Principales ataques sobre una sesión

Métodos

- Los diferentes tipos de malware normalmente intentan aprovechar algún tipo de agujero o vulnerabilidad del sistema (o de las personas que lo utilizan):
  - *Exploit*
  - Desbordamiento de memoria o *buffer overflow*
  - *Core dumps*
  - Inyección de código o *code injection*:
    - SQL injection
    - Cross site scripting
    - ...
  - Ingeniería social
  - Phishing

Principales ataques sobre una sesión

Contramedidas

- Instalar antivirus/antispyware en las estaciones de trabajo
- Mantener el sistema operativo correctamente actualizado
- Mantener las aplicaciones correctamente actualizadas
- Utilizar de software de fuentes confiables
- Establecer una política de mínimos privilegios
- Estar al corriente de las posibles vulnerabilidades
- Instalar un sistema de detección de rootkits, intrusos, modificación inadecuada de binarios, ...