Hacking ético

Módulo 0

Introducción al Hacking Etico

Objetivos

- Introducir el hacking ético y terminología esencial.
- Entender las diferentes fases seguidas por un hacker
- Revisión de los hackers y crackers más famosos

¿Puede ser ético el Hacking?

- El nombre *hacker – neologismo utilizado para referirse a un experto (Gurú) en varias o alguna rama técnica relacionada con las tecnologías de la información y las telecomunicaciones: programación, redes, sistemas operativos.*
- Cracker – (criminal hacker, 1985). *Un cracker es alguien que viola la seguridad de un sistema informático de forma similar a como lo haría un hacker, sólo que a diferencia de este último, el cracker realiza la intrusión con fines de beneficio personal o para hacer daño a su objetivo.*

¿Puede ser ético el Hacking?

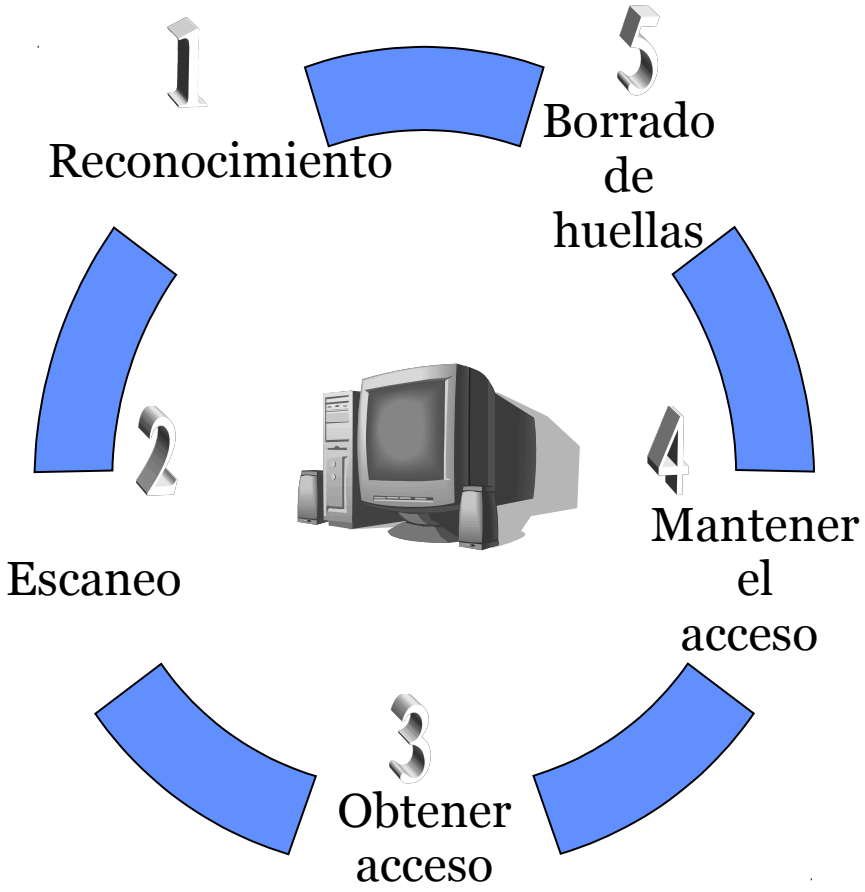
- Hacker ético – profesionales de la seguridad que aplican sus conocimientos de hacking con fines defensivos (y legales).
- Diremos hacker siempre, pero hay que fijarse en el contexto.

Elementos de seguridad

- Elementos esenciales de la seguridad.
- Confidencialidad – tiene que ver con la ocultación de información o recursos.
- Autenticidad - es la identificación y garantía del origen de la información.
- Integridad - Se refiere a cambios no autorizados en los datos.
- Disponibilidad – Posibilidad de hacer uso de la información y recursos deseados.

¿Qué puede hacer un hacker?

- Reconocimiento
  - Pasivo
- Rastreo (*escaneo*)
  - Activo
- Acceso
  - Sistema operativo / aplicación
  - Redes
  - Denegación de servicio
- Mantener el acceso
- Borrado de huellas



Fase 1 - Reconocimiento

- Previo a cualquier ataque
- Información sobre el objetivo.
- Reconocimiento pasivo:
  - Google Hacking
  - Ingeniería social
  - Monitorización de redes de datos. Por ejemplo, sniffing, etc.

Fase 2 - Escaneo

- Escaneo es una fase de pre-ataque.
- Se escanea la red pero ya con información de la fase previa
- Detección de vulnerabilidades y puntos de entrada.
- El escaneo puede incluir el uso de escaneadores de puertos y de vulnerabilidades.

Fase 1 - Escaneo (cont.)

- Reconocimiento activo – Probar la red para detectar
  - hosts accesibles
  - puertos abiertos
  - localización de routers
  - Detalles de sistemas operativos y servicios

Fase 3 – Ataque. Obtener acceso

- Obtención de acceso – Se refiere al ataque propiamente dicho.
- Por ejemplo, hacer uso de un exploit o bug
  - Obtener una password, ataques man-in-the_middle (spoofing), exploits (buffer overflows), DoS (denial of service).

Fase 4 – Ataque. Mantener acceso

- Mantenimiento del acceso- se trata de retener los privilegios obtenidos.
- A veces un hacker blinda el sistema contra otros posibles hacker, protegiendo sus puertas traseras, rootKits y Troyanos.

Fase 5 – Borrado de huellas

- Borrado de huellas – se intenta no ser descubierto.
- Hay que tener claro que hay técnicas más intrusivas (y por lo tanto delatoras) que otras.
- Análisis forense

Tipos de Hacker

- **Black hats**
  - Individuals with extraordinary computing skills, resorting to malicious or destructive activities. Also known as ‘Crackers.’
- **White Hats**
  - Individuals professing hacker skills and using them for defensive purposes. Also known as ‘Security Analysts’.
- **Gray Hats**
  - Individuals who work both offensively and defensively at various times.

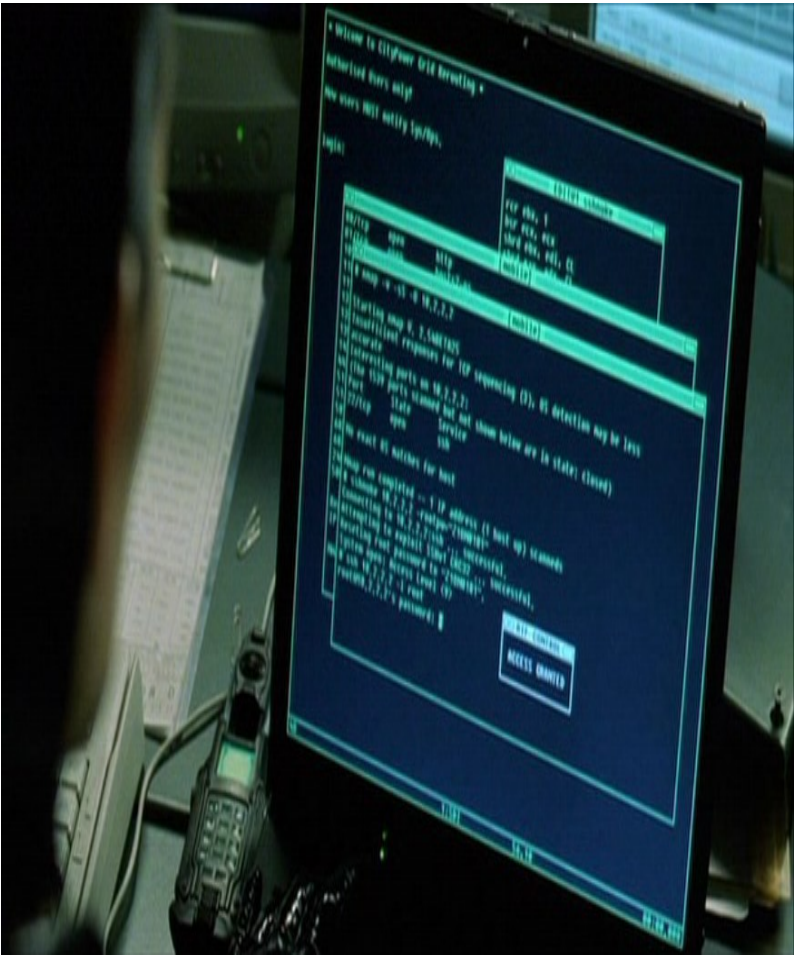
Hacktivismo

- Se refiere a ‘hacking por una causa’.
- Es el compromiso político o social del haking
- Por ejemplo, atacar y alterar sitios web por razones políticas, tales como ataques a sitios web del gobierno o de grupos que se oponen a su ideología.
- Pero hay acciones que son delito (tengan o no una justificación idelológica)

¿Qué puede hacer un hacker ético?

- "*If you know the enemy and know yourself, you need not fear the result of a hundred battles.*"
  - *Sun Tzu,* Art of War
- Un hacker ético intenta responder a las siguientes preguntas:
  - ¿Qué puede saber un intruso de su objetivo? Fases 1 y 2
  - ¿Qué puede hacer un intruso con esa información? Fases 3 y 4
  - ¿Se podría detectar un intento de ataque? Fases 5 y 6
- ¿Para que querría una empresa contratar a un haker ético?

Perfil de habilidades de un hacker ético



- Experto en algún campo de la informática.
- Conocimientos profundos de diversas plataformas (Windows, Unix, Linux).
- Conocimientos de redes
- Conocimientos de hardware y software.

¿Qué debe hacer un hacker ético?

- Fases de un proceso de evaluación de la seguridad:
- Preparación – Se debe tener un contato firmado por escrito donde se exonere al hacker ético de toda responsabilidad como consecuencia de las pruebas que realice (siempre que sea dentro del marco acordado)
- Gestión – Preparación de un informe donde se detallen las pruebas y posibles vulnerabilidades detectadas.
- Conclusión – Comunicación a la empresa del informe y de las posibles soluciones.

Modos de Hacking Etico

- Redes remotas – Simulación de un ataque desde Internet.
- Redes locales – Simulación de un ataque desde dentro (empleados, hacker que ha obtenido privilegios en un sistema,...)
- Ingeniería social – Probar la confianza de los empleados.
- Seguridad física – Accesos físicos (equipos, cintas de backup,...)

Evaluando la seguridad

- Tipos de tests de seguridad
- Black-box (sin conocimiento de la infraestructura que se está evaluando)
- White-box (con un conocimiento completo de la infraestructura que se está evaluando).
- Test interno (se le conoce también como *Gray-box testing*) – se examina la red desde dentro.

¿Qué se debe entregar ?

- Ethical Hacking Report
- Detalles de los resultados de las actividades y pruebas de hacking realizadas. Comparación con lo acordado previamente en el contrato.
- Se detallarán las vulnerabilidades y se sugiere cómo evitar que hagan uso de ellas.
- ¡Ojo, que esto debe ser absolutamente confidencial!
- Deben quedar registrados en el contrato dichas cláusulas de confidencialidad.

Hackers famosos

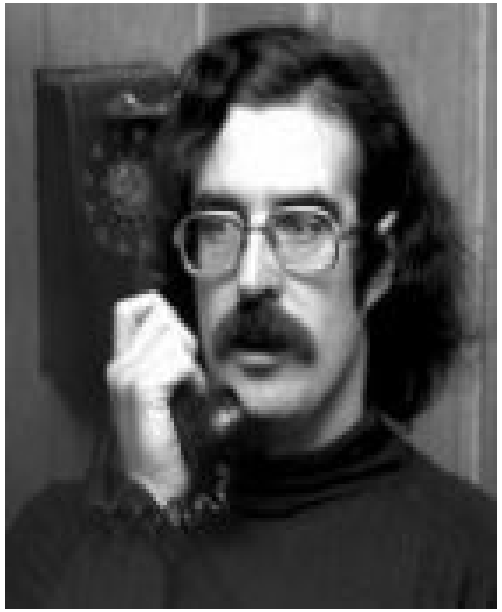
- Paul Baram – el primer haker de la historia y el que creó el concepto de hacker.
- Kevin David Mitnick es el hacker más famoso de los últimos tiempos. En 1992 el gobierno acusó a Kevin de haber substraído información del FBI. Mitnick fue arrestado por el FBI en Raleigh, North Carolina, el 15 de Febrero de 1995. Ahora tiene una empresa de seguridad: http://www.kevinmitnick.com/

Hackers famosos

- Mark Abene más conocido como Phiber Optik. Lideró en New York, al grupo de hackers denominado "Master of Deception", MOD (Maestros de la Decepción).
- En Noviembre de 1989, hizo colapsar las computadoras de WNET, uno de los principales canales de televisión de la ciudad de New York, dejando un mensaje "Happy Thanksgiving you turkeys, from all of us at MOD" (Feliz Día de Acción de Gracias a Uds. pavos, de parte de todos nosotros en MOD).

Hackers famosos

- John Draper (EUA)
- Prácticamente un ídolo de los tres anteriores, introdujo el concepto de Phreaker, al conseguir realizar llamadas gratuitas utilizando un pito de plástico que venia de regalo en una caja de cereales. Obligó a los EUA a cambiar de señalización de control en sus sistemas de telefonía.



Hackers famosos

- Chen Ing-Hou es el creador del virus Chernobyl en 1998
- Johan Helsingius es el responsable de Remailer, uno de los más famosos servidores de mail anónimo.
- El servidor Remailer, no almacena los mensajes sino que sirve como un canal de re-transmisión de los mismos. El Remailer re-envía estos mensajes, sin dar a conocer la identidad del remitente original.
- Sir Dystic es el hacker autor del programa original Back Orifice,

Hackers famosos

- David L. Smith es sospechoso de ser el autor del virus Melissa.
- Tsutomu Shimomura buscó, encontró y desenmascaró a Kevin Mitnick a principios de 1994, y que previamente había entrado en su ordenador robándole ficheros.
- ElGranOscarín, hacker español y autor del troyano Cabronator. Las iniciales son O.L.H y que en los primeros días de Abril del 2003 fue detenido por la Guardia Civil.
  - http://elgranoscarin.cjb.net/
  - MSN-Phuk (carga cuentas de Hotmail ajenas), ANONIMIZAME (proxy anónimo)

Los hackers más famosos