Hacking ético

Tema 0

Introducción al Hacking Etico

Objetivos

- Introducir el hacking ético y terminología esencial.
- Entender las diferentes fases seguidas por un hacker

¿Puede ser ético el Hacking?

- El nombre *hacker* es un *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.*

¿Puede ser ético el Hacking?

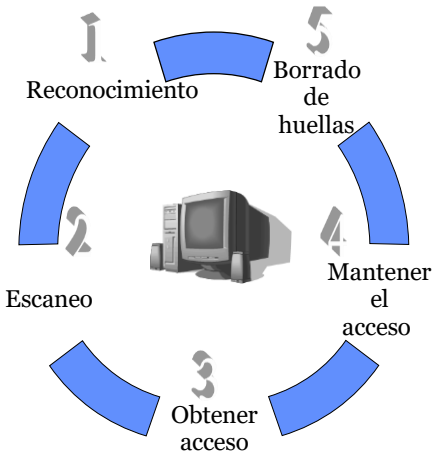
- Cracker – (criminal hacker, 1985). *Un cracker es alguien que viola la seguridad de un sistema informático de forma similar a como lo haría un hacker*
- *Sólo que a diferencia de este último, el cracker realiza la intrusión con fines de beneficio personal o para hacer daño a su objetivo.*

¿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.

¿Qué puede hacer un hacker?

- Reconocimiento
- Escaneo
- Acceso - Ataque
  - *A nivel de* sistema operativo / aplicación
  - Redes
  - Denegación de servicio
- Mantener el acceso
- Borrado de huellas



Fase 1 - Reconocimiento

- Previo a cualquier ataque
- Recopilar información sobre el objetivo de forma legal

Fase 2 - Escaneo

- Seguimos recopilando información sobre el objetivo
- Reconocimiento activo:
  - Monitorización de redes de datos (normalmente mediante sniffers)
  - Escaneo de vulnerabilidades

Fase 2 - Escaneo

- Se escanea la red pero ya con información de la fase previa(fase 1)
- Y esto ya es ilegal
- Necesitaremos por lo tanto un permiso para hacerlo

Fase 3 - Gaining Access (obtener acceso)

- Obtención de acceso – Se refiere al ataque propiamente dicho.
- Por ejemplo, hacer uso de un exploit o bug
- El atacante puede obtener acceso a nivel de sistema operativo, de aplicación o de red.

Fase 4 – Mantener acceso

- Mantenimiento del acceso- se trata de retener los privilegios obtenidos.
- Eso se hace dejando instaladas puertas traseras (backdoors), 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.
- Esto da lugar a otra rama de la seguridad – Informática 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.

Tipos de Hacker

- **Script kiddies**
- Esto es lo que no queremos ser

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?

- 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? Fase 5

¿Qué puede hacer un hacker ético?

- ¿Para que querría una empresa contratar a un haker ético?
- ¿Y hay ofertas de trabajo para los hackers éticos?
- Ver infojobs

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?

- Su herramienta: penetration testing (pentesting)

¿Qué debe hacer un hacker ético?

- **Penetration testing**
- Es un método para evaluar la seguridad de un sistema o red simulando un ataque para encontrar vulnerabilidades que un atacante podría explotar

¿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 (pentesting)
- 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 con información parcial.

¿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.

¿Qué se debe entregar ?

- ¡Ojo, que esto debe ser absolutamente confidencial!
- Deben quedar registrados en el contrato dichas cláusulas de confidencialidad.

Resumen del proceso