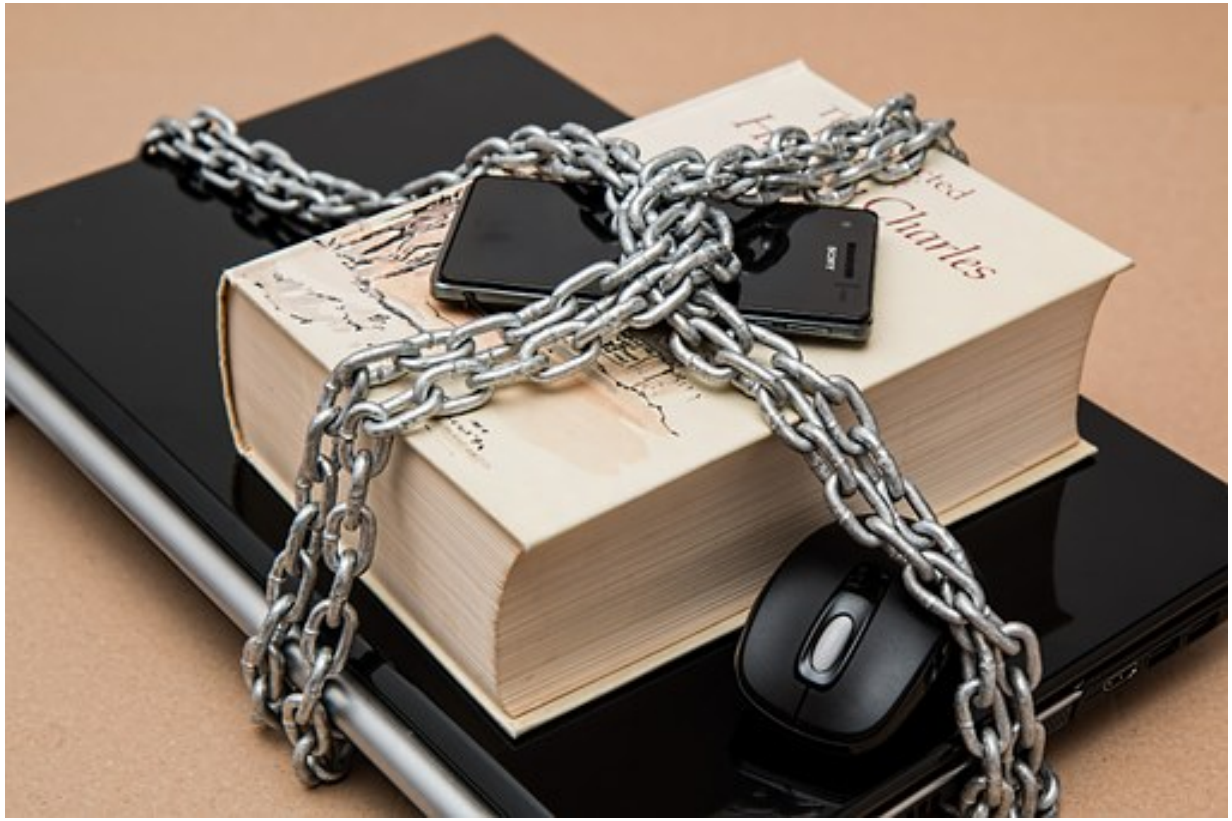
Capítulo 8: Seguridad en redes



Contenido de esta clase

- Fundamentos de la seguridad
- Un poco de historia de la seguridad informática
- Línea de Tiempo
- Definición de la Seguridad
- Conceptos y terminología de seguridad
- Gerencia de la seguridad de la información
- Hackeo ético
  - Reconocimiento
  - Escáneo
  - Tomar control
  - Mantener control
  - Limpieza de trazas

Hackeo ético: tomar control

Crackeo de credenciales

* Para tomar el control de sistema el hacker debe vulnerar las contraseñas de los usuarios que logró encontrar, para ello hará uso de alguna de las siguientes técnicas:
  - Ataque en línea pasivo o activo
  - Ataque fuera de línea
  - Ataque no electrónico

Hackeo ético: tomar control

Crackeo de credenciales

* Un ataque típico para romper las contraseñas son aquellos realizados fuera de línea y que utilizan algún archivo encontrado por el hacker en dónde se encuentren las contraseñas cifradas
  - Para descifrarlas se utilizan herramientas cómo Jack The Ripper que con tiempo y buenos diccionarios se realiza un ataque de fuerza bruta combinando la permutación de caracteres y palabras comunes o “por omisión” utilizadas en paquetes de instalación

Hackeo ético: mantener control

Rootkits

- Luego de lograr el acceso el hacker tratará de escalar privilegios y ejecutar aplicaciones o exploits de forma encubierta.
- Una forma común de encubrimiento son los rootkits.
- Los rootkits se instalan en el kernel y tienen la habilidad de esconderse y encubrir sus actividades.
- Cuando se instala un rootkit se reemplazan llamados del sistema operativo por versiones o rutinas modificadas que contienen la ejecución de script o aplicación adicional al llamado natural que realiza la función.
- Un rootkit puede: Esconder procesos, archivos, entradas en el registro interceptar comandos, solicitar debug (causando los famosos pantallazos azules), redirigir archivos .exe, etc.

Hackeo ético: mantener control

Contramedidas para los rootkits

- Cuando un rootkit se instala en un sistema operativo, es prácticamente imposible deshacerte de él por completo. Por lo que el sistema operativo resultante es poco confiable
- Por ello lo mejor es evitarlos, existen herramientas en diferentes sistemas operativos para detectarlos al momento que se está intentado instalar: Blacklight, Rootkit revealer
- Determinar los archivos críticos, bases de datos, librerías, que necesitas respaldar ya que respaldar regularmente todo el disco te hará vulnerable a rootkits.

Hackeo ético: limpieza de trazas

* Un hacker experimentado al finalizar un ataque intentará limpiar sus pasos antes de dejar el equipo.
  - Limpiar, borrar los logs o registros del sistema
  - Limpiar los comandos cómo history

* Utilizar herramientas automatizadas para tal fin como:
  - Elsave
  - Evidence eliminator
  - Traceless
  - Winzapper