Importante: Para los ejercicios 4, 5 y 6, puede ser útil descargar diccionarios de palabras. Puede buscar algunos en:
https://github.com/danielmiessler/SecLists/tree/master/Passwords
http://contest-2010.korelogic.com/wordlists.html

EJERCICIO 1

Un desarrollador de una aplicación web debe diseñar y programar el módulo de autenticación de un sistema de control de reactores nucleares. Se ve frente a las siguientes opciones para almacenar las contraseñas en una base de datos:

- En texto claro
- Cifradas con AES y una clave fija
- "Hasheadas" con SHA-1

Explique cuáles son los problemas con cada uno de los métodos anteriores y los posibles ataques, si es que los hubiere. De haberlos, explique el diseño de un algoritmo que no presente las mismas debilidades ni sea vulnerable a los mismos ataques.

EJERCICIO 2

Las bases de datos Oracle soportan un mecanismo de autenticación llamado "remote OS authentication" que permite delegar la autenticación del usuario a un sistema operativo remoto. Es decir, permite que el usuario Pompin autenticado en un sistema operativo remoto se conecte a través de la red a la base de datos sin proveer credenciales (asumiendo que el usuario Pompin existe en la base de datos y está configurada su cuenta para autenticación remota).

¿Cuál es el problema de seguridad que presenta este mecanismo? Si tuviese un aplicativo que no funciona si no se habilita este mecanismo de autenticación para un usuario particular en la base de datos, ¿cómo haría para proteger esta cuenta?

EJERCICIO 3

Los servicios/comandos "r" utilizan el servicio Identd (TCP/113) para autenticar al usuario. ¿Qué mecanismo de seguridad del sistema operativo es el que impide que un atacante, con acceso como usuario no privilegiado a un servidor con relación de confianza con otro servidor, ejecute un demonio Identd que falsifique las respuestas para obtener acceso al servidor con el cual existe la relación de confianza? ¿Cómo podría un atacante falsificar la respuesta del demonio Identd?

EJERCICIO 4

El archivo parcial_1c2008.doc contiene un parcial antiguo de la materia, cifrado. Utilice John the ripper jumbo y sus herramientas asociadas para descifrar el archivo y acceder al enunciado del parcial. Investigue si hubiese sido más difícil obtener la contraseña si se hubiese usado una versión más moderna de Office para generar el documento.

EJERCICIO 5

El archivo capitulo1.zip contiene el primer capítulo de un libro muy famoso. Descifre los archivos para ver de que libro se trata.

EJERCICIO 6

Intente recuperar las contraseñas que corresponden a los hashes incluidos en el archivo hashes.txt. Puede usar john the ripper o hashcat. Analice el tiempo que lleva, según el tipo de función de hash utilizada.