**Hacking**

**Ético**

# Hacking Máquina

# Windows 7

### 

| Enunciado |
| --- |
| Sobre la máquina Windows 7, y siempre de forma remota, atacando desde un Kali Linux, realizar los primeros intentos de Pentesting:  Obtener la mayor información posible de la máquina víctima:   * Vulnerabilidades encontradas. Intentar explotar alguna vulnerabilidad. * Acceder aprovechando malas configuraciones y posibles debilidades para comprometer la máquina. * Se debe finalmente poder contestar a las siguientes preguntas. * ¿Quién es un enchufado del Director? |
| * Puertos abiertos. * Servicios encontrados. * Sistema Operativo. |
|  |
|  |
| Sesión abierta de ftp, con credenciales de mysql. |
| -sC → corre diferentes scripts de reconocimiento por defecto |
| Probaré a explotar el servicio http |
| Con **whatweb** nos devuelve información relevante |
|  |
| Se puede obtener también con |
| **Curl -s -X GET -I http://10.0.2.6** |
|  |
|  |
| El método TRACE está habilitado. |
| RACE allows the client to see what is being received at the other end of the request chain and use that data for testing or diagnostic information. |
| No encuentro campo de input para intentar un ataque xss. |
| Utilizó el archivo encontrado en el servidor ftp para acceder a la base de datos |
|  |
| Con el usuario “ana”, logro enumerar los usuarios y sus contraseñas en hash. |
| Modifico la consulta para obtener un formato usable por jhon the ripper |
|  |
|  |
| Esta version usa **mysql\_native\_password** |
| Se continúa con la explotación en clase. |