**Parte 4.2 Cursos no gratuitos sobre la tecnología Aircrack-NG**

**4.2.1 Curso no gratuito 1 sobre Aircrack-NG**

Este curso, es en modalidad online, lo imparten profesionales muy reconocidos en el mundo de la seguridad informática como son las personas que forman parte de la comunidad dragonjar. Ofrecen un contenido que se van actualizando constantemente. Entre esos contenidos se encuentra el de “Ataques actuales para redes inalámbricas” en el que se utiliza, entre otras, la herramienta Aircrack –NG.

El precio de este curso no es una cantidad en concreto, sino que es una suscripción anual de 1000 USD/año, por ello, los contenidos se van actualizando constantemente.

Enlace: <https://www.dragonjar.education/diplomado/>

**4.2.2 Curso no gratuito 2 sobre Aircrack-NG**

En este online que se imparte gracias a la página web [www.pentestmag.com](http://www.pentestmag.com), se explica como hacer un test de seguridad en pentesting de redes Wi-Fi como un profesional. En el segundo modulo del curso, se estudia la herramienta Aircrack-NG.

Este curso no tiene un precio en concreto, sino que la pagina tiene la política de que cada usuario page una suscripción anual de 790 USD/año para que puedan acceder a los contenidos de este curso y de los demás cursos que imparten.

Enlace: <https://pentestmag.com/course/advanced-wireless-penetration-testing-15-2/>

**4.2.3 Curso no gratuito 3 sobre Aircrack-NG**

Este curso lo imparte el Digital Tech Institute, está diseñado para empresas que quieran invertir en la formación de sus empleados y aumentar sus conocimientos en seguridad informática y hacking ético. En el módulo 4, de hacking ético, hay un apartado sobre ataques en redes inalámbricas, en el que se utilizara la herramienta Aircrack-NG.

Enlace: <http://www.digitaltechinstitute.com/formacion-in-company/itinerario-seguridad-it/#1484231461750-d6d95da4-788c>

**4.2.4 Curso no gratuito 4 sobre Aircrack-NG**

En este curso se explican muchos conceptos sobre los protocolos y sistemas de las redes inalámbricas y como hacer tests de penetración en función de esos protocolos y sistemas. Para ello, entre otras herramientas, utilizan la herramienta Aircrack-NG.

Enlace: <https://backtrackacademy.com/curso/hacking-wireless>