# Nikto

## ¿Qué es? ¿Para qué sirve?

Nikto es una herramienta para el escaneo de vulnerabilidades en servidores web que fue lanzada como versión beta el 27 de diciembre de 2001. Su software es Open Source y poco a poco ha ido consiguiendo mayor éxito en el mundo del pentesting hasta convertirse en el escáner de vulnerabilidades web gratuito más popular. Su nombre hace referencia a la película “The Day the Earth Stood Still”.

## ¿Cómo funciona?

Para llevar a cabo su propósito, Nikto realiza una serie de actividades entre las que destacan: escaneo de vulnerabilidades y malas configuraciones, identificación del software instalado y detección de problemas específicos de la versión del servidor, análisis y búsqueda de ficheros en instalaciones por defecto, búsqueda de programas predeterminados e inseguros, etc.

## Usando Nikto

Para mostrar el uso de esta herramienta voy a utilizar una máquina virtual con un Kali Linux para hacer de atacante y un servidor web Metaesploitable como el que hemos utilizado en clase de prácticas que va a ser atacado.

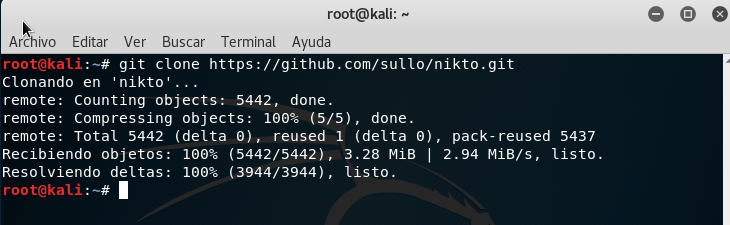
Para empezar a usar Nikto va a ser necesario tener instalado en nuestra máquina:

* Perl
* Openssl
* Libnet-ssley-perl
* Nmap

En mi caso no hizo falta realizar ninguna instalación ya que todos los programas anteriores venían ya por defecto.

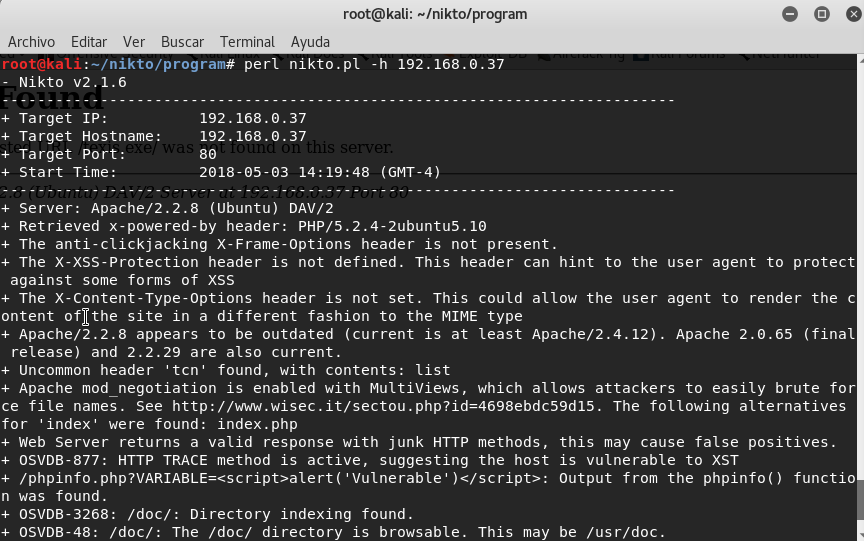
Una vez tengamos instalados los requisitos iniciales podemos optar por instalar Nikto mediante la orden “apt-get install nikto” o bien clonar su repositorio oficial de GitHub en nuestra máquina Kali y trabajar sobre él. Esta última opción ha sido por la que yo me he decantado ya que en un primer intento la otra me dio varios problemas.

* Clonamos el repositorio:



En este punto ya podemos empezar a trabajar con la herramienta. Para familiarizarnos un poco con ella vamos a realizar un ataque básico sobre nuestra máquina Metaesploitable con ip 192.168.0.37 .

* Nos situamos sobre la carpeta /nikto/program y ejecutamos la orden:
  + perl nikto.pl -h 192.168.0.37



En este ataque básico por defecto que hemos utilizado podemos observar en la imagen de arriba, el puerto sobre el que se ha realizado el ataque ha sido el 80. A simple vista nos llaman la atención cosas como el tipo de servidor que se está utilizando y en qué versión (Apache 2.2.8) o la versión de PHP que está utilizando (5.2.4) . Los datos que acabamos de obtener con una simple orden nos pueden ser de gran utilidad a la hora de realizar un ataque y a su vez ofrecen una clara idea sobre el potencial de esta herramienta.