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

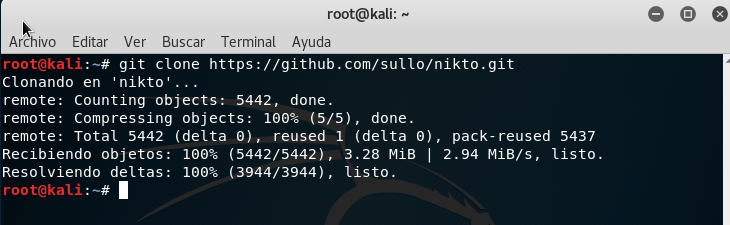
Para empezar a usar Nikto va a ser necesario tener instalado en nuestra máquina:

* 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 escaneo 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

Imagen que contiene captura de pantalla

Descripción generada con confianza muy alta

En este escaneo 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 cierta información que se muestra como el tipo de servidor que se está utilizando y en qué versión (Apache 2.2.8), su sistema operativo (Ubuntu) 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.

CONTINUARÁ …

# NmapImagen que contiene objeto, mesa, interior Descripción generada con confianza alta

## ¿Qué es? ¿Para qué sirve?

Nmap es una de las herramientas más importantes en el mundo del pentesting y la seguridad informática. Tiene como propósito explorar, administrar y auditar la seguridad de las redes de equipos informáticos ofreciendo un informe detallado al usuario que lo utiliza. Fue lanzada al público el 1 de septiembre de 1997 y al igual que Nikto, es una herramienta Open Source y además se encuentra regulada por una Licencia Pública General GNU. Cabe destacar que Nmap es multiplataforma, por lo que existe una versión para la mayoría de los sistemas operativos que conocemos.

## ¿Cómo funciona?

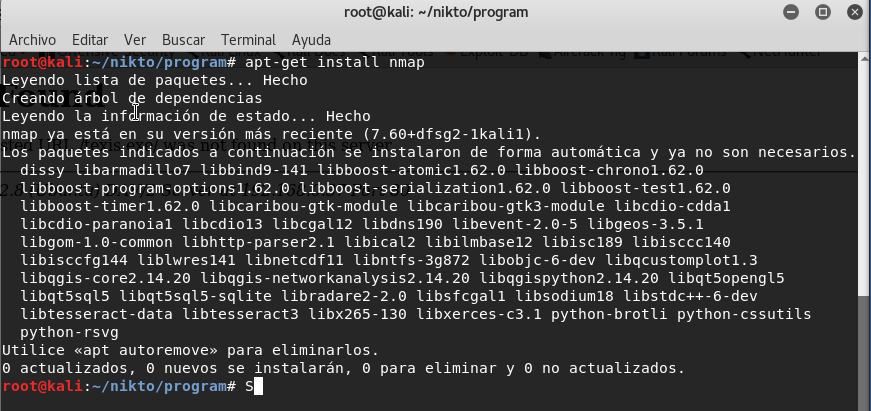
Nmap realiza un escaneo aprovechándose de los paquetes IP crudos, es decir, los que aún no han sufrido ningún tipo de modificación, para ofrecer al usuario un análisis en profundidad donde podemos encontrar información de gran utilidad como, por ejemplo, los equipos que se encuentran en una determinada red, así como los servicios que ejecutan, sus sistemas operativos, sus puertos abiertos, si usan cortafuegos, etc.

## Usando Nmap

Para mostrar el funcionamiento de esta herramienta me voy a apoyar en una máquina Kali simulando ser un atacante y un servidor Web Metasploitable que va a ser atacado al igual que anteriormente.

En este caso voy a instalar Nmap con una orden directamente y sin necesidad de haber instalado nada previamente.

* apt-get install nmap



Como podemos observar, una herramienta tan importante como es nmap, ya viene instalada por defecto en nuestro sistema Kali.

A continuación, nos disponemos a realizar un escaneo básico sobre nuestro servidor Metasploitable. Para ello simplemente ejecutamos el siguiente comando:

* nmap 192.168.0.37

Imagen que contiene texto

Descripción generada con confianza muy alta

Como podemos observar, el resultado ha sido satisfactorio, ya que hemos encontrado un montón de puertos abiertos que nos pueden resultar de gran utilidad. A simple vista nos puede llamar la atención algunos servicios que se están ejecutando en dichos puertos como, por ejemplo, ssh, rpcbind, nfs, postgrsql… Con esta información ya tendríamos un amplio abanico de opciones por las que decantarse a la hora de realizar un ataque.