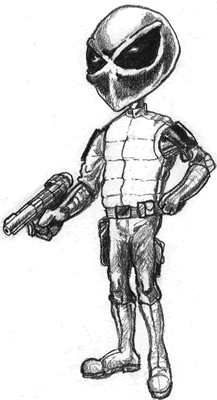
Nikto y nmap

Imagen que contiene objeto, mesa, interior

Descripción generada con confianza alta

Pablo Menéndez Suárez 71899158P UO252406

Escuela de Ingeniería informática – Seguridad de Sistemas Informáticos

03/05/2018

**Índice**

[**Nikto** 2](#_Toc513294082)

[¿Qué es? ¿Para qué sirve? 2](#_Toc513294083)

[¿Cómo funciona? 2](#_Toc513294084)

[Usando Nikto 2](#_Toc513294085)

[**Nmap** 7](#_Toc513294086)

[¿Qué es? ¿Para qué sirve? 7](#_Toc513294087)

[¿Cómo funciona? 7](#_Toc513294088)

[Usando Nmap 8](#_Toc513294089)

[Datos de interés 11](#_Toc513294090)

[**Nikto+Nmap** 12](#_Toc513294091)

[Combinar Nikto y Nmap 12](#_Toc513294092)

[Uso de Nikto y Nmap 12](#_Toc513294093)

[¿Son legales Nikto y Nmap? 12](#_Toc513294094)

# 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.

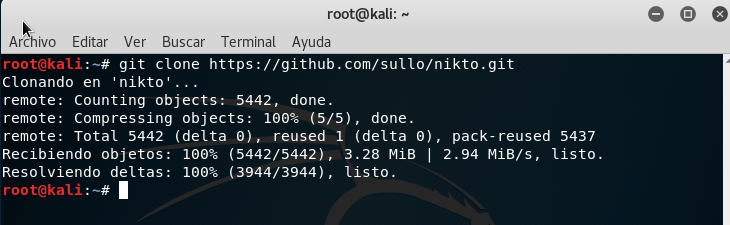
Para empezar a usar Nikto va a ser necesario tener instalado en nuestra máquina:

* 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 .

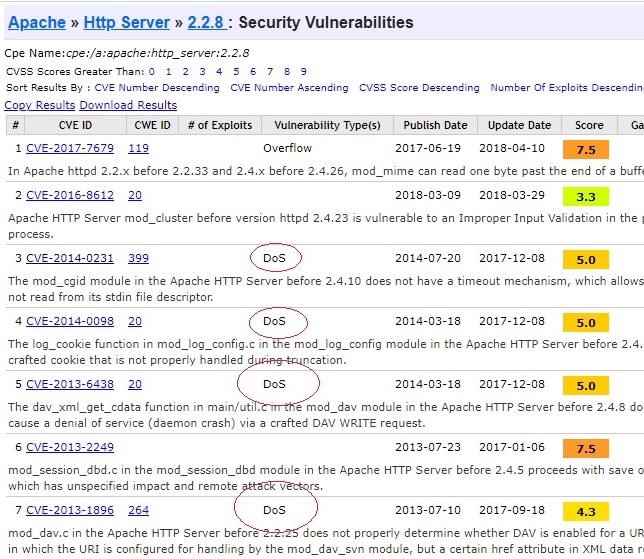
* Nos situamos sobre la carpeta /nikto/program y ejecutamos la orden:
  + perl nikto.pl -h 192.168.0.37

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.

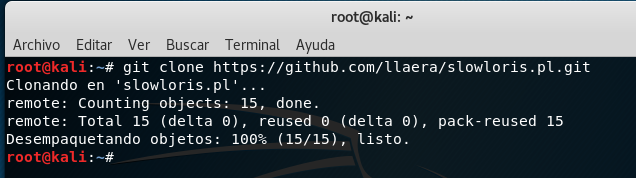
Vamos a aprovecharnos de los datos obtenidos para intentar realizar un ataque sobre nuestro servidor Metasploitable. Para ello, a través de la web “www.cvedetails.com” he realizado una búsqueda de vulnerabilidades del servidor Apache 2.2.8 y los resultados han sido los siguientes:



Como podemos observar, parece que el servidor Apache 2.2.8 es bastante vulnerable frente a ataques DOS, es decir, frente a ataques de denegación de servicios, por lo que vamos a intentar realizar uno de ellos.

Investigando un poco más sobre estos ataques he conseguido un pequeño programa en Python conocido como “Slowloris” que nos permitirá realizar un ataque de denegación de servicios sobre servidores que no tengan un mecanismo de “time out”, como es en este caso nuestro servidor Apache 2.2.8. Clonamos el repositorio donde se encuentra alojado el programa.

* git clone https://github.com/llaera/slowloris.pl.git

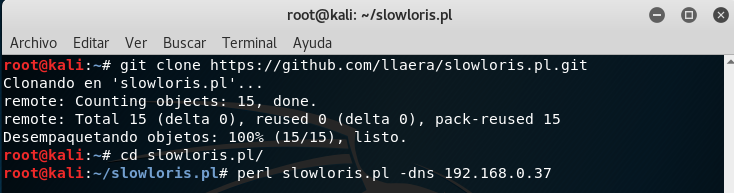


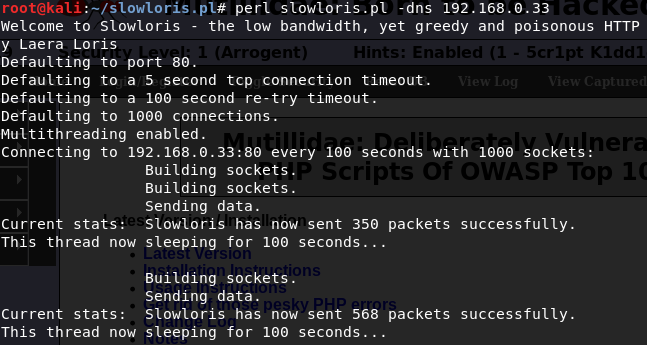
Nos situamos sobre el directorio Slowloris.pl ya estamos listos para realizar el ataque. Antes de realizarlo, verificamos que la web funciona correctamente. A partir de este punto, la IP de mi máquina Metasploitable ha pasado a ser 192.168.0.33 debido a que he tenido que realizar un cambio de equipo.

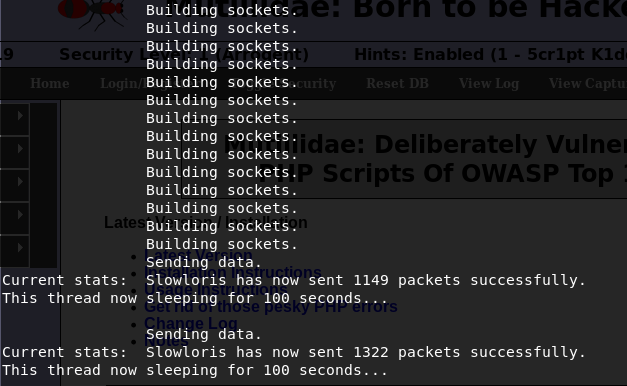


Una vez verificamos que la web funciona correctamente realizamos el ataque mediante la orden:

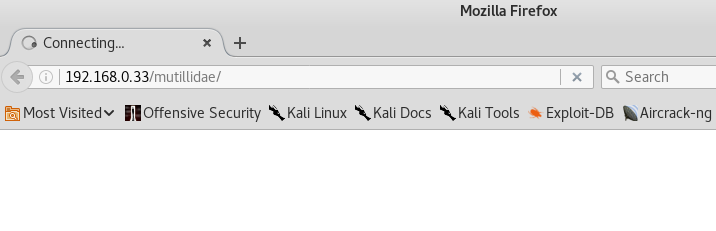
* perl slowloris.pl -dns 192.168.0.33







Cada 100 segundos el programa se está conectando a nuestro servidor mediante 1000 sockets. Si nos intentamos conectar ahora a nuestro servidor web, el resultado es el siguiente:



Como podemos observar, sus servicios han caído. La web se actualiza constantemente pero nunca llega a mostrarnos nada. Todo esto ha sido posible gracias a la herramienta Nikto que nos ha simplificado enormemente el trabajo a la hora de buscar vulnerabilidades para nuestra máquina Metasploitable. Sin la información proporcionada por Nikto, el ataque hubiera sido mucho más costoso ya que tendríamos que ir probando hasta dar con uno que funcionase.

# 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?

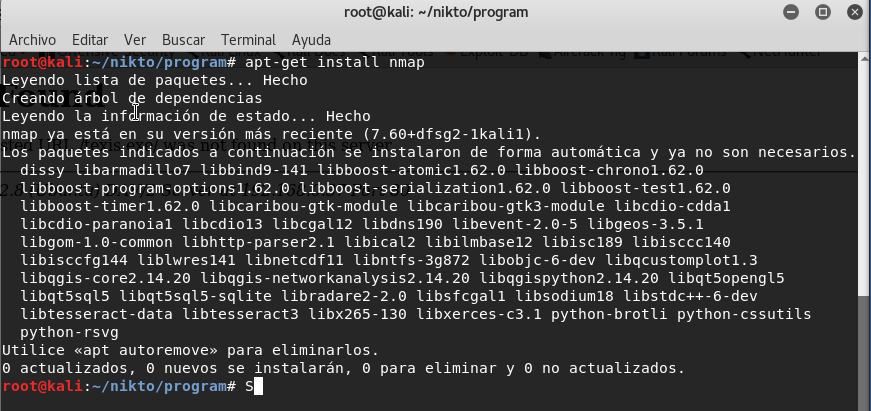
Nmap realiza un escaneo aprovechándose de los paquetes IP crudos, es decir, los que aún no han sufrido ningún tipo de modificación, para ofrecer al usuario un análisis en profundidad donde podemos encontrar información de gran utilidad como, por ejemplo, los equipos que se encuentran en una determinada 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.

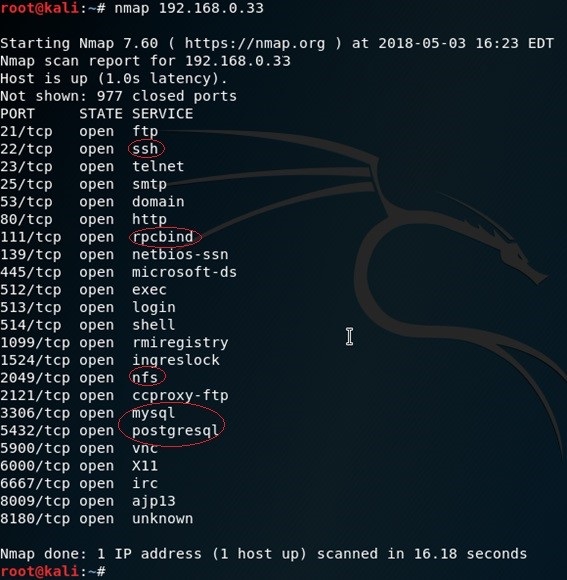
En este caso voy a instalar Nmap con una orden directamente y sin necesidad de haber instalado nada previamente.

* apt-get install nmap



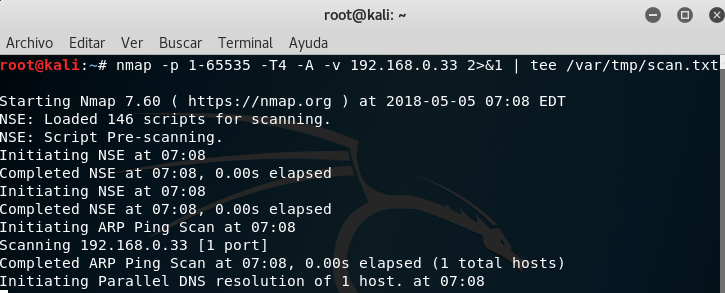
Como podemos observar, una herramienta tan importante como es nmap, ya viene instalada por defecto en nuestro sistema Kali. A continuación, nos disponemos a realizar un escaneo básico sobre nuestro servidor Metasploitable. Para ello simplemente ejecutamos el siguiente comando:

* nmap 192.168.0.33



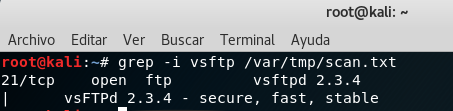
Como podemos observar, el resultado ha sido satisfactorio, ya que hemos encontrado un montón de puertos abiertos que nos pueden resultar de gran utilidad. A simple vista nos puede llamar la atención algunos servicios que se están ejecutando en dichos puertos como, por ejemplo, ssh, rpcbind, nfs, postgrsql…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

En mi caso, voy a optar por realizar un escaneo un poco más complejo sobre nuestra máquina objetivo. Mediante el comando “nmap -p 1-65535 -T4 -A -v 192.168.0.33 2>&1 | tee /var/tmp/scan.txt” vamos a realizar un escaneo agresivo para intentar averiguar el sistema operativo, la versión y sus puertos abiertos entre otras características, guardando el resultado en el fichero “scan.txt” alojado en el directorio “/var/tmp”.

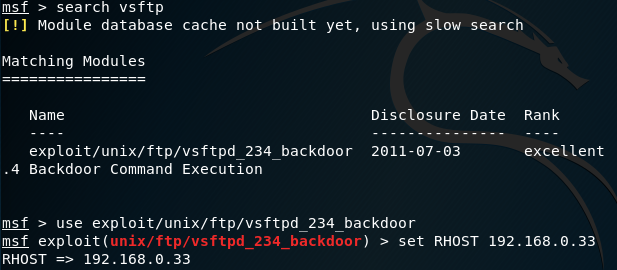


Para realizar el ataque, voy a intentar aprovecharme de un fallo de seguridad que posee el servidor “vsftp”, pero, antes de nada, debemos verificar que este servicio se está ejecutando sobre nuestra máquina Metasploitable y que además su puerto está abierto. Para ello vamos a realizar un filtrado del fichero obtenido.

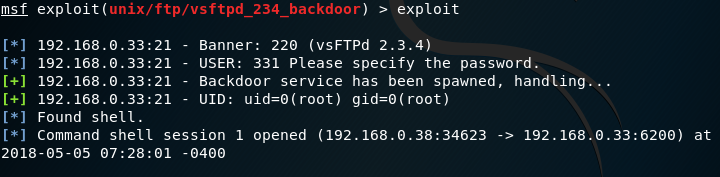
* grep -i vsftp /var/tmp/scan.txt



A la vista de los resultados obtenidos, sabemos que dicho servicio se está ejecutando sobre nuestra máquina objetivo en el puerto abierto 21, por lo que podemos continuar con nuestro ataque. Vamos a aprovecharnos del framework “Metasploit” para realizar el ataque automáticamente y de manera más sencilla. Buscamos el exploit que necesitamos mediante la orden “search vsftp” y una vez obtenida su localización configuramos los datos del host de la víctima.

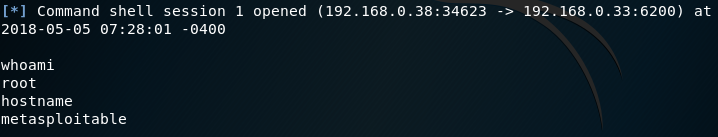


Una vez esté todo listo, ejecutamos la orden “exploit” y procedemos con el ataque.



Como podemos observar, hemos abierto una puerta trasera desde nuestra máquina Kali a la máquina Metasploitable. Y no solo eso, si no que además tenemos permisos de superusuario sobre la otra máquina. Comprobamos que esto es cierto:

* whoami
* hostname

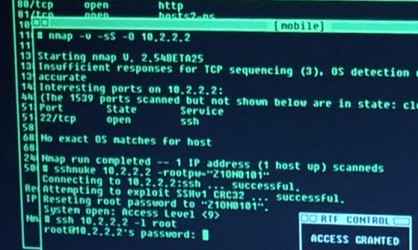


Una vez llegado a este punto, la lista de cosas que podríamos hacer es muy amplia, desde cambiarle la contraseña al super usuario, meter nuestra clave pública en su fichero de authorized\_keys, crear un usuario dentro de la máquina, etc.

## Datos de interés

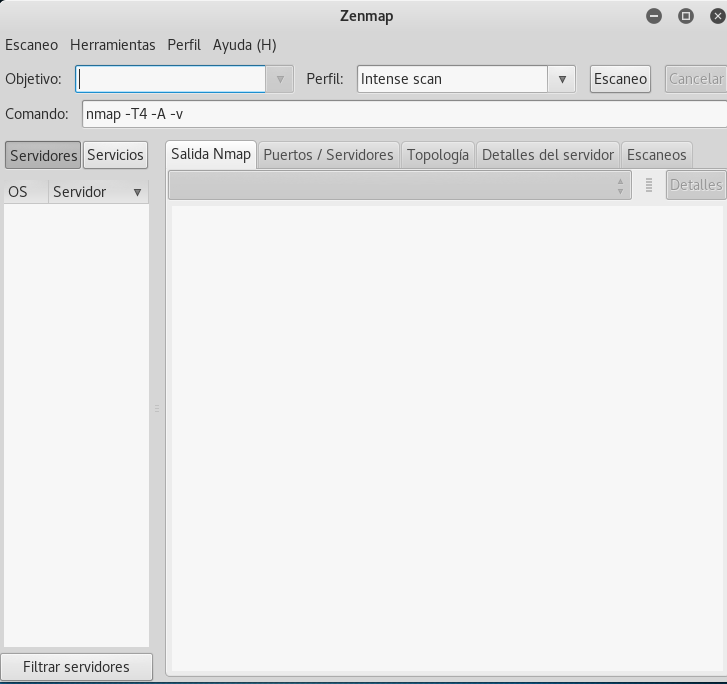
Nmap ha sido utilizado en algunas películas en las que se simulaban ataques a otras máquinas. Sin embargo, con la película “The Matrix Reloaded” convirtió a Nmap realmente en una estrella de cine.





Aquí podemos ver a “Tríniti”, un personaje de la película, realizando un escaneo con Nmap a otro equipo.

Cabe destacar también, que Nmap dispone también de una versión gráfica conocida como ZenMap. Tiene un aspecto similar al siguiente:



# Nikto+Nmap

## Combinar Nikto y Nmap

Estas dos herramientas pueden ser usadas de manera conjunta para obtener mejores resultados. Por ejemplo, podemos utilizar esta orden:

* nmap -p80 192.168.0.33 -oG - | perl nikto-pl -h –

De esta manera conseguimos que Nmap busque servidores http en el puerto 80 de la máquina y se los pasa a Nikto para que los analice.

## Uso de Nikto y Nmap

Tanto Nmap como Nikto pueden ser usadas para bien o para mal. Muchos expertos en seguridad informática se aprovechan de estas herramientas para buscar fallos de seguridad en sus equipos, ya que ambas lo único que hacen es realizar un escaneo, pero nunca llegan más allá, es decir, nunca explotan las vulnerabilidades que encuentran a no ser que sean complementadas con otras herramientas. De manera análoga, muchos ciberdelincuentes utilizan dichas herramientas para encontrar vulnerabilidades en servidores ajenos y así tener más oportunidades a la hora de lanzar un ataque.

## ¿Son legales Nikto y Nmap?

A la hora de usar cualquiera de estas herramientas debemos tener sumo cuidado, ya que lanzar un escaneo a un servidor ajeno sin ningún tipo de permiso es un delito. Sin embargo, podemos utilizarlas sin temor alguno contra una de nuestras máquinas.

# Bibliografía

* https://cirt.net/Nikto2
* https://thehackerway.com/2011/05/12/conceptos-basicos-de-nikto-tecnicas-de-escaneo-de-servidores-y-aplicaciones-web/
* https://github.com/sullo/nikto
* https://elbinario.net/2016/09/16/niktoescaner-de-vulnerabilidades-web/
* https://www.hackingtutorials.org/web-application-hacking/scanning-webservers-vulnerabilities-with-nikto/
* https://es.wikipedia.org/wiki/Nmap
* https://paraisolinux.com/que-es-y-como-usar-nmap/
* https://nmap.org/man/es/index.html#man-description
* https://seguinfo.wordpress.com/2007/06/27/%C2%BFque-es-nmap/
* http://recursostic.educacion.es/observatorio/web/es/component/content/article/1050-zenmap?start=1
* https://metasploit.help.rapid7.com/docs/metasploitable-2-exploitability-guide
* https://computersecuritystudent.com/SECURITY\_TOOLS/METASPLOITABLE/EXPLOIT/lesson8/index.html
* https://github.com/llaera/slowloris.pl