NIKTO

What is Nikto?

It's a web vulnerability scanner written in perl and licensed under the GPL. It will allow you to test the security of your web server configuration (HTTP options, indexes, potential XSS vulnerabilities, SQL injections etc...).

Disclaimer

Use only on your own servers. The scan generates several lines in the logs with your IP in the apache logs or in any IDS. The interest is to find flaws at home to be able to secure our web servers.

Installation

I use Kali linux for this tutorial, by default Nikto is available in it. On other distributions you have to download it from safe sources.

Example sources:

https://github.com/sullo/nikto

https://github.com/sullo/nikto/archive/master.zip

Scanning WEB ports (80 and 443)

By default Nikto scans on port 80 so let's see how to scan HTTPS port 443 instead :

```
Kali@kali:~$ nikto -h https://[URL]:443/ -F txt -o ScanResultat.txt
```

Scan multiports

```
Kali@kali:~$ nikto -h https://[URL] -p 8080,80,443
```

Scan multihosts

It is possible to scan a range of web server addresses. Nikto is able to read on its standard input. So, we give it the result of a nmap scan :

```
kali@kali:~$ nmap -p 80 x.x.x.x/24 -oG – | nikto.pl -h –
```

Proxy scan

If you want to do the tests through a proxy, you will have to add the configuration in the Nikto configuration file:

```
# Proxy settings -- still must be enabled by -useproxy

PROXYHOST= ip_or_url_du_proxy

PROXYPORT=8080

#PROXYUSER=proxyuserid

#PROXYPASS=proxypassword
```

```
Kali@kali:~$ nikto -h https://[URL] -useproxy
```

Verbose and debug scan

```
Kali@kali:~$ nikto -h https://[URL] -p 80,443 -D -v
```

Useful links :

source: http://cirt.net/nikto2
doc: http://cirt.net/nikto2-docs/usage.html