Nikto is one of the most popular web server scanners designed to fingerprint and test web servers for a variety of possible weaknesses including potentially dangerous files and out-of-date versions of applications and libraries. It is written in the Perl language.
Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/programs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software. Scan items and plugins are frequently updated and can be automatically updated.

Nikto is not designed as a stealthy tool. It will test a web server in the quickest time possible and is obvious in log files or to an IPS/IDS. However, there is support for LibWhisker's anti-IDS methods in case you want to give it a try (or test your IDS system).

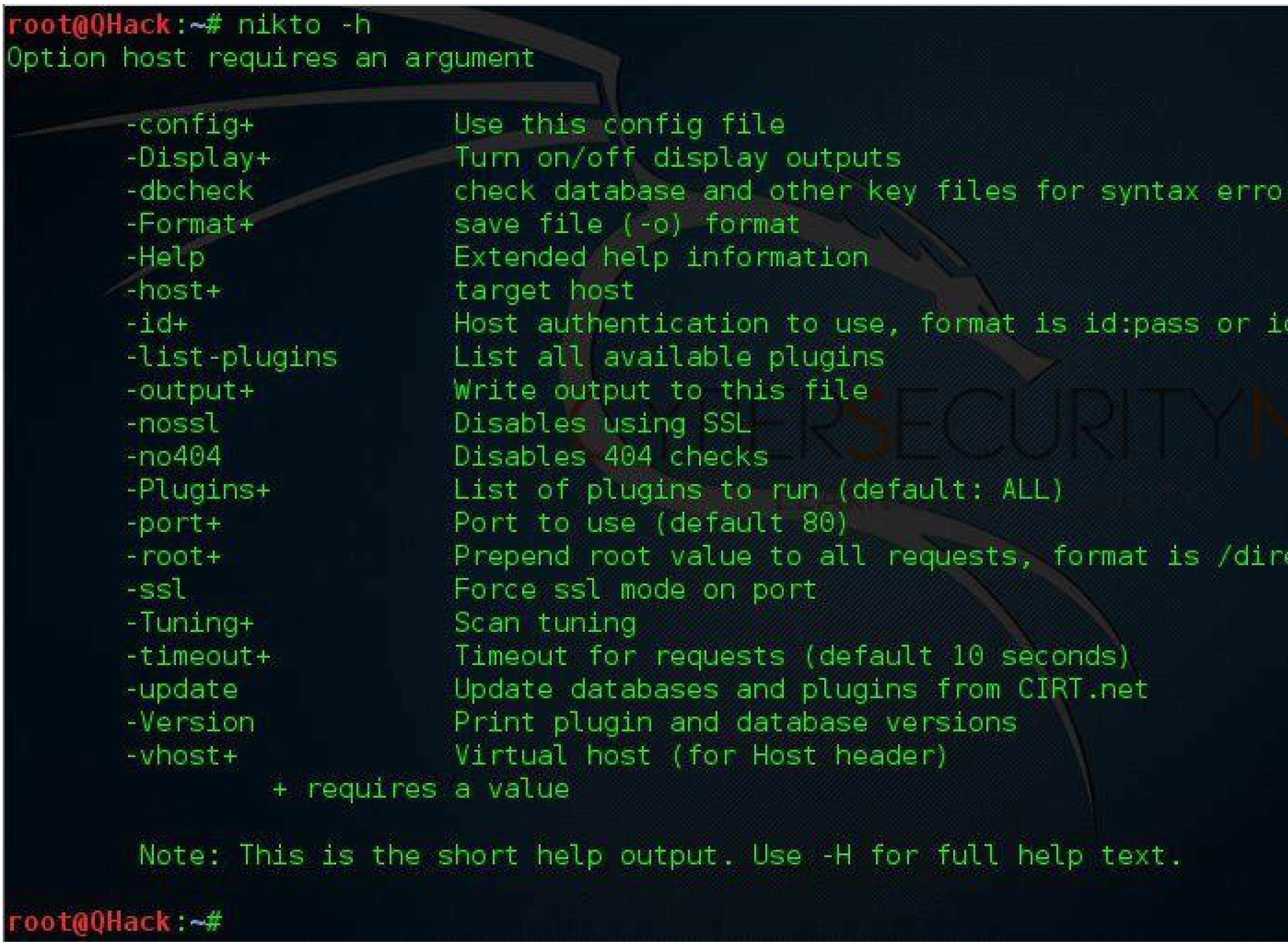
Features of Nikto Web Scanner

- • SSL Support (Unix with OpenSSL or maybe Windows with ActiveState's Perl/NetSSL)
  • Full HTTP proxy support
  • Checks for outdated server components
  • Save reports in plain text, XML, HTML, NBE or CSV
  • Template engine to easily customize reports
  • Scan multiple ports on a server, or multiple servers via input file (including nmap output)
  • LibWhisker's IDS encoding techniques
  • Easily updated via command line
  • Identifies installed software via headers, favicons and files
  • Host authentication with Basic and NTLM
  • Subdomain guessing
  • Apache and cgiwrap username enumeration
  • Mutation techniques to "fish" for content on web servers
  • Scan tuning to include or exclude entire classes of vulnerability checks
  • Guess credentials for authorization realms (including many default id/pw combos)
  • Authorization guessing handles any directory, not just the root directory
  • Enhanced false positive reduction via multiple methods: headers, page content, and content hashing
  • Reports "unusual" headers seen
  • Interactive status, pause and changes to verbosity settings
  • Save full request/response for positive tests
  • Replay saved positive requests
  • Maximum execution time per target
  • Auto-pause at a specified time
  • Checks for common "parking" sites
  More detail go for original documentation page https://cirt.net/nikto2-docs/

How do I use a Nikto web Scanner to scan the Website?

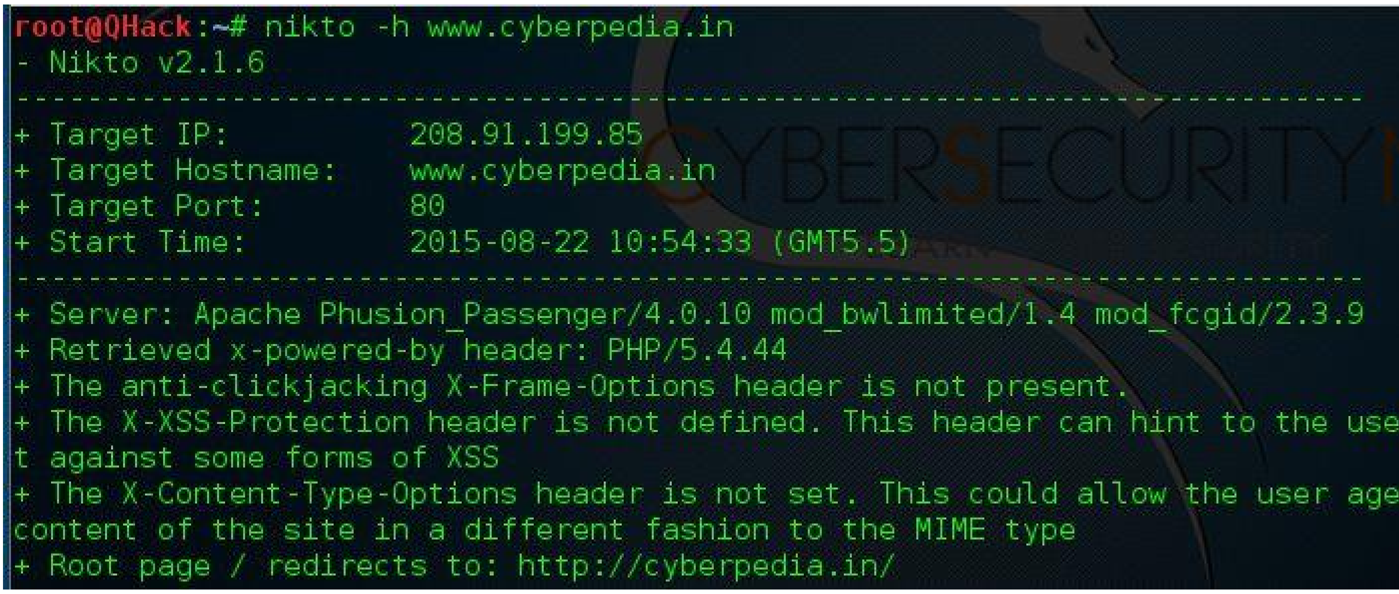
Run Nikto

The most basic Nikto scan requires simply a host to target, since port 80 is assumed if none is specified. The host can either be an IP or a hostname of a machine, and is specified using the -h (-host) option. This will scan the IP 192.168.0.1 on TCP port 80:
#nikto -h



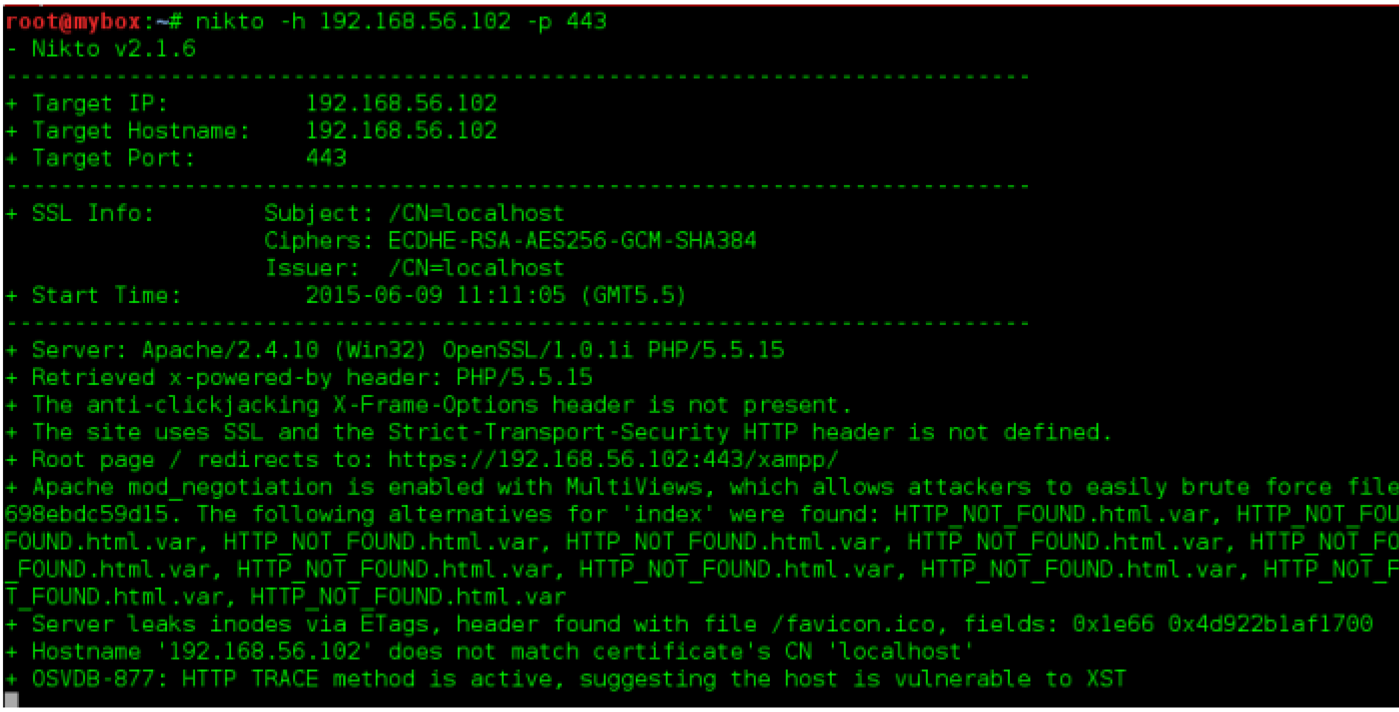
```
root@QHack:~# nikto -h
Option host requires an argument

       -config+            Use this config file
       -Display+           Turn on/off display outputs
       -dbcheck            check database and other key files for syntax erro
       -Format+            save file (-o) format
       -Help               Extended help information
       -host+              target host
       -id+                Host authentication to use, format is id:pass or i
       -list-plugins       List all available plugins
       -output+            Write output to this file
       -nossl              Disables using SSL
       -no404              Disables 404 checks
       -Plugins+           List of plugins to run (default: ALL)
       -port+              Port to use (default 80)
       -root+              Prepend root value to all requests, format is /dir
       -ssl                Force ssl mode on port
       -Tuning+            Scan tuning
       -timeout+           Timeout for requests (default 10 seconds)
       -update             Update databases and plugins from CIRT.net
       -Version            Print plugin and database versions
       -vhost+             Virtual host (for Host header)
               + requires a value

        Note: This is the short help output. Use -H for full help text.

root@QHack:~#
```

#nikto -h www.cyberpedia.in



```
root@QHack:~# nikto -h www.cyberpedia.in
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          208.91.199.85
+ Target Hostname:    www.cyberpedia.in
+ Target Port:        80
+ Start Time:         2015-08-22 10:54:33 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache Phusion_Passenger/4.0.10 mod_bwlimited/1.4 mod_fcgid/2.3.9
+ Retrieved x-powered-by header: PHP/5.4.44
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the use
t against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user age
content of the site in a different fashion to the MIME type
+ Root page / redirects to: http://cyberpedia.in/
```

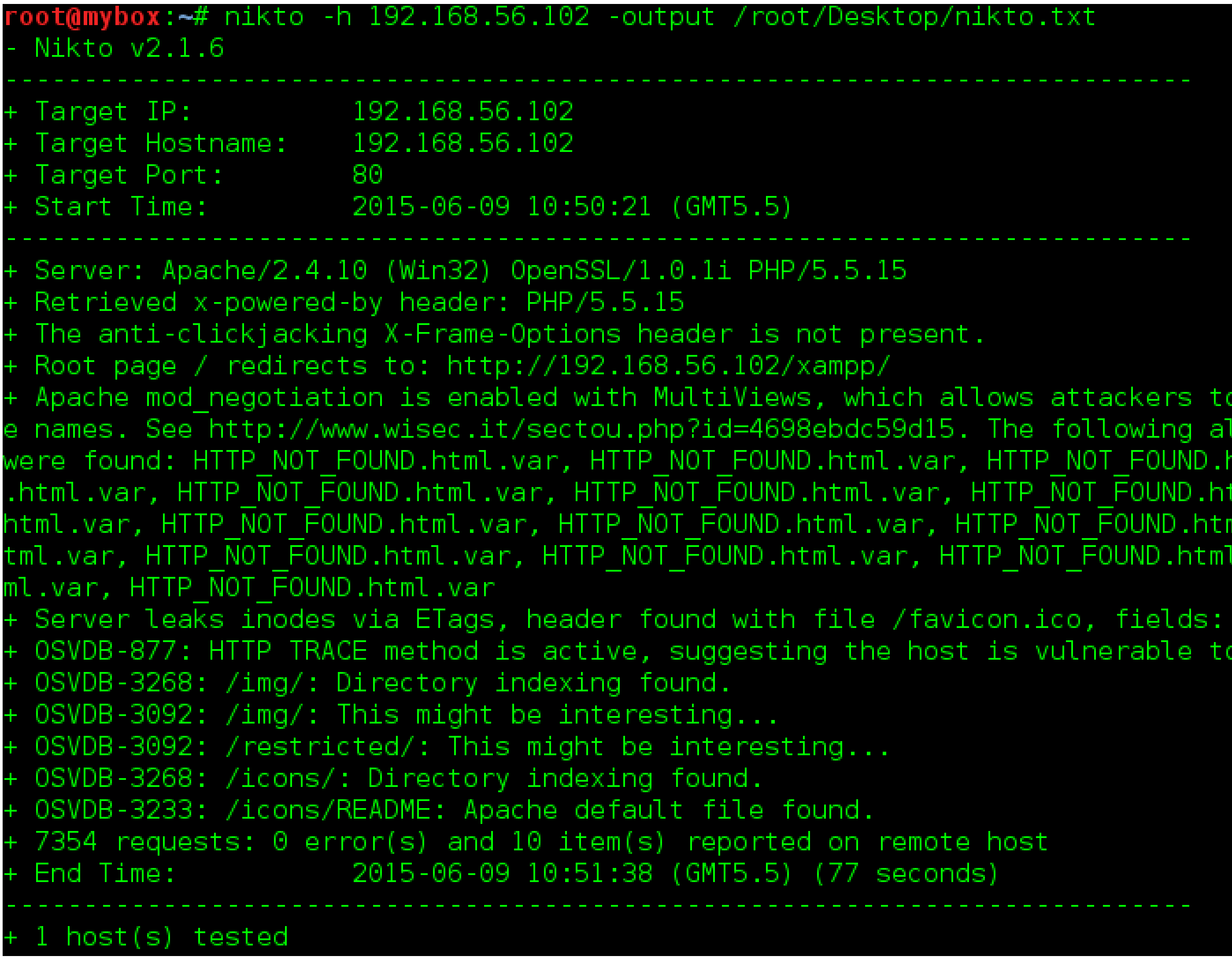
To check on a different port, specify the port number with the -p (-port) option. This will scan the IP 192.168.0.1 on TCP port 443:
#nikto -h 192.168.56.102 -p 443
Hosts, ports and protocols may also be specified by using a full URL syntax, and it will be scanned:
#nikto -h https://192.168.56.102:443/



```
root@mybox:~# nikto -h 192.168.56.102 -p 443
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.56.102
+ Target Hostname:    192.168.56.102
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject: /CN=localhost
                   Ciphers: ECDHE-RSA-AES256-GCM-SHA384
                   Issuer:  /CN=localhost
+ Start Time:         2015-06-09 11:11:05 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.10 (Win32) OpenSSL/1.0.1i PHP/5.5.15
+ Retrieved x-powered-by header: PHP/5.5.15
+ The anti-clickjacking X-Frame-Options header is not present.
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ Root page / redirects to: https://192.168.56.102:443/xampp/
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file
698ebdc59d15. The following alternatives for 'index' were found: HTTP_NOT_FOUND.html.var, HTTP_NOT_FOU
FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FO
_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_F
T_FOUND.html.var, HTTP_NOT_FOUND.html.var
+ Server leaks inodes via ETags, header found with file /favicon.ico, fields: 0x1e66 0x4d922b1af1700
+ Hostname '192.168.56.102' does not match certificate's CN 'localhost'
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
```

There is no need to specify that port 443 may be SSL, as Nikto will first test regular HTTP and if that fails, HTTPS. If you are sure it is an SSL server, specifying -s (-ssl) will speed up the test.
#nikto -h 192.168.56.102 -p 443 -ssl

There is one option to save scan report into the file with the difference-2 format, for example, xml txt CSV, etc
#nikto -h 192.168.56.102 –output /root/Destop/nikto.txt



```
root@mybox:~# nikto -h 192.168.56.102 -output /root/Desktop/nikto.txt
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.56.102
+ Target Hostname:    192.168.56.102
+ Target Port:        80
+ Start Time:         2015-06-09 10:50:21 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.10 (Win32) OpenSSL/1.0.1i PHP/5.5.15
+ Retrieved x-powered-by header: PHP/5.5.15
+ The anti-clickjacking X-Frame-Options header is not present.
+ Root page / redirects to: http://192.168.56.102/xampp/
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to
e names. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following al
were found: HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.h
.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.ht
html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.htm
tml.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html.var, HTTP_NOT_FOUND.html
ml.var, HTTP_NOT_FOUND.html.var
+ Server leaks inodes via ETags, header found with file /favicon.ico, fields:
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to
+ OSVDB-3268: /img/: Directory indexing found.
+ OSVDB-3092: /img/: This might be interesting...
+ OSVDB-3092: /restricted/: This might be interesting...
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 7354 requests: 0 error(s) and 10 item(s) reported on remote host
+ End Time:           2015-06-09 10:51:38 (GMT5.5) (77 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Nikto can scan multiple ports in the same scanning session. To test more than one port on the same host, specify the list of ports in the -p (-port) option. Ports can be specified as a range (i.e., 80-90), or as a comma-delimited list, (i.e., 80,88,90). This will scan the host on ports 80, 88 and 443.
#nikto -h 192.168.56.102 -p 80,88,443
Nikto support scanning multiple hosts in the same session via a text file of hostnames or IPs. Instead of giving a hostname or IP for the -h (-host) option, a file name can be given. A file of hosts must be formatted as one host per line, with the port number(s) at the end of each line. Ports can be separated from the host and other ports via a colon or a comma. If no port is specified, port 80 is assumed.