# nikto cheat sheet

comparitech

| | |
|---|---|
| Installation | `$ sudo apt-get install nikto` |
| Standard command to scan websites | `nikto -host (web url host name) -(http port number )` |

## Scan options

| | |
|---|---|
| Nikto -h (Hostname/IP address) | Scan a host |
| Nikto -h -port (Port Number1),(Port Number2) | Scan host targeting specific ports |
| Nikto -h (Hostname) -maxtime (seconds) | Define maximum scan time |
| Nikto -h-until | Scan duration |
| Nikto -h-vhost | Define host header |
| Nikto -h-no404 | Skip http 404 guessing |
| Nikto -h-nossl | Stop using SSL during scan |
| Nikto -h-ssl | Force to use SSL |
| Nikto -update | Update scan engine plugins |
| Nikto -h-dbcheck | Check database |
| Nikto -h (Hostname/IP address) -output (filename) | Input output to a file |
| Nikto -h-useproxy (Proxy IP address) | Web host scan via a proxy |
| Nikto -h-config (filename.conf) | Use a specified file as a database |
| Nikto -h-nolookup | Stop DNS lookup for hosts |
| Nikto -h-nocache | Stop caching responses for scans |

## Display Options

`Nikto -h -Display (option)`

| | |
|---|---|
| 1 | Display redirects |
| 2 | Display cookies |
| 3 | Display 200 ok response |
| 4 | Display Web URLs requiring authentication |
| D | Display debug output |
| E | Show HTTP errors |
| P | Print to STDOUT |
| V | Verbose output display |

## Output Options

`Nikto -h -Format`

| | |
|---|---|
| csv | Comma Separated Value |
| htm | HTML Format |
| txt | Plain text |
| xml | XML Format |

## Tuning Options

`Nikto -h (Hostname) -tuning (Option)`

| | | | |
|---|---|---|---|
| 0 | Upload files | 7 | Remote File Retrieval - Server Wide |
| 1 | View specific file in log | 8 | Command Execution / Remote Shell |
| 2 | DDefault file misconfiguration | 9 | SQL Injection |
| 3 | Display information disclosure | a | Authentication Bypass |
| 4 | Injection (XSS/Script/HTML) | b | Software Identification |
| 5 | Remote File Retrieval - Inside Web Root | c | Remote Source Inclusion |
| 6 | Denial of Service | x | Reverse Tuning Options |

Reference and additional resources - https://github.com/sullo/nikto