**🔎 Nikto Web Vulnerability Scanner – Cheat Sheet**

**📌 Overview**

Nikto is an **open-source web server scanner** that detects:

* Dangerous files & outdated software
* Default installations & misconfigurations
* Security issues like XSS, SQLi, command execution

**⚙️ Basic Syntax**

nikto -h <target>

Example:

nikto -h http://192.168.1.10

**🚀 Common Commands**

**1. Scan a Host**

nikto -h http://example.com

**2. Scan with HTTPS**

nikto -h https://example.com

**3. Specify Port**

nikto -h example.com -p 8080

**4. Scan Multiple Ports**

nikto -h example.com -p 80,443,8080

**5. Use an Input File (Multiple Targets)**

nikto -h targets.txt

**🎯 Advanced Usage**

**1. Use SSL Explicitly**

nikto -h example.com -ssl

**2. Verbose Output**

nikto -h example.com -Display V

**3. Save Output to File**

nikto -h example.com -o result.txt

**4. Export in HTML, CSV, or XML**

nikto -h example.com -Format html -o result.html

nikto -h example.com -Format csv -o result.csv

nikto -h example.com -Format xml -o result.xml

**5. Evade IDS/IPS with Delay**

nikto -h example.com -delay 10

**6. Specify a User-Agent**

nikto -h example.com -useragent "Mozilla/5.0"

**7. Enable/Disable SSL Certificate Checking**

nikto -h example.com -ssl -nocheck

**📋 Useful Options**

| **Option** | **Description** |
| --- | --- |
| -h | Target host or file |
| -p | Specify port(s) |
| -ssl | Force SSL usage |
| -o | Save output |
| -Format | Output format (txt, html, xml, csv) |
| -Tuning | Choose type of scan (files, injections, etc.) |
| -useragent | Set custom User-Agent |
| -Plugins | Run specific plugins |
| -Cgidirs | Scan specific CGI directories |

**🎛 Tuning Options (-Tuning)**

| **Number** | **Scan Type** |
| --- | --- |
| 0 | File Upload |
| 1 | Interesting Files |
| 2 | Misconfigurations |
| 3 | Information Disclosure |
| 4 | Injection (SQL, Command, etc.) |
| 5 | Remote File Retrieval |
| 6 | Denial of Service |
| 7 | Remote Source Inclusion |

Example:

nikto -h example.com -Tuning 1234

**💡 Pro Tips**

* Always run with different -Tuning options for deeper scans
* Combine with **Nmap** or **Dirb** for comprehensive web recon
* Use -o with multiple formats for better reporting
* Add delay when scanning sensitive systems to avoid detection