cd into your nikto git clone directory:

```
git pull
```

Main script is in program

```
cd nikto/program
```

Check out the 2.5.0 branch

```
git checkout nikto-2.5.0
```

Run using the shebang interpreter

```
./nikto.pl -h http://www.foo.com
```

Run using perl (if you forget to chmod)

```
perl nikto.pl -h http://www.foo.com
```

- list element with functor item

Nikto Scan Cheat Sheet

The following Nikto command usage for scanning a web application:

COMMAND	DESCRIPTION
`nikto -h http://foo.com`	Scans the specified host
`nikto -h http://foo.com -Tuning 6`	Uses a specific Nikto scan tuning level
`nikto -h http://foo.com -port 8000`	Scans the specified port
`nikto -h http://foo.com -ssl`	Scans for SSL vulnerabilities

Commands & Examples
Subfinder Cheat Sheet
Naabu Cheat Sheet: Commands & Examples
Reverse Shell Cheat Sheet: PHP, ASP, Netcat, Bash & Python
DNS Tunneling dnscat2 Cheat Sheet
SSH Lateral Movement Cheat Sheet
Android Pen Testing Environment Setup
Password Reset Testing Cheat Sheet
SSRF Cheat Sheet & Bypass Techniques
Pen Testing Tools Cheat Sheet
LFI Cheat Sheet
Vim Cheat Sheet [2022 Update] + NEOVIM
Systemd Cheat Sheet
nbtscan Cheat Sheet
Linux Commands Cheat Sheet
More »

COMMAND	DESCRIPTION
`nikto -h http://foo.com -Format html`	Formats output in HTML
`nikto -h http://foo.com -output out.txt`	Saves the output to a file

Nikto Command Flags Sheet

The following Nikto commands allow for configuration of a Nikto scan:

OPTION	VALUE
`-ask+`	`yes` Ask about each (default) `no` Don't ask, don't send
`-Cgidirs+`	"none", "all", or values like "/cgi/ /cgi-a/"
`-config+`	Use this config file
`-Display+`	1 Show redirects 2 Show cookies received 3 Show all 200/OK responses 4 Show URLs which require authentication D Debug output E Display all HTTP errors P Print progress to STDOUT S Scrub output of IPs and hostnames V Verbose output
`-dbcheck`	Check database and other key files for syntax errors
`-evasion+`	1 Random URI encoding (non-UTF8) 2 Directory self-reference (/./) 3 Premature URL ending 4 Prepend long random string 5 Fake parameter 6 TAB as request spacer 7 Change the case of the URL 8 Use Windows directory separator (\) A Use a carriage return (0x0d) as a request spacer

WALKTHROUGHS

InsomniHack CTF Teaser - Smartcat2 Writeup
InsomniHack CTF Teaser - Smartcat1 Writeup
FristiLeaks 1.3 Walkthrough
SickOS 1.1 - Walkthrough
The Wall Boot2Root Walkthrough
More »

TECHNIQUES

SSH & Meterpreter Pivoting Techniques
More »

SECURITY HARDENING

Security Harden CentOS 7
More »

/DEV/URANDOM

MacBook - Post Install Config + Apps
More »

OPTION	VALUE
	B Use binary value 0x0b as a request spacer
`-Format+`	csv Comma-separated-value htm HTML Format msf+ Log to Metasploit nbe Nessus NBE format txt Plain text xml XML Format (if not specified the format will be taken from the file extension passed to -output)
`-Help`	Extended help information
`-host+`	Target host
`-IgnoreCode`	Ignore Codes--treat as negative responses
`-id+`	Host authentication to use, format is id:pass or id:pass:realm
`-key+`	Client certificate key file
`-list-plugins`	List all available plugins, perform no testing
`-maxtime+`	Maximum testing time per host
`-mutate+`	1 Test all files with all root directories 2 Guess for password file names 3 Enumerate user names via Apache (/~user type requests) 4 Enumerate user names via cgiwrap (/cgi-bin/cgiwrap/~user type requests) 5 Attempt to brute force sub-domain names, assume that the host name is the parent domain 6 Attempt to guess directory names from the supplied dictionary file
`-mutate-options`	Provide information for mutates
`-nointeractive`	Disables interactive features
`-nolookup`	Disables DNS lookups

OTHER BLOG

Insecure Direct Object Reference (IDOR): Definition, Examples & How to Find
HowTo: Kali Linux Chromium Install for Web App Pen Testing
Jenkins RCE via Unauthenticated API
MacBook - Post Install Config + Apps
enum4linux Cheat Sheet - Commands & Examples
Linux Local Enumeration Script

OPTION	VALUE
`-nossl`	Disables the use of SSL
`-no404`	Disables nikto attempting to guess a 404 page
`-output+`	Write output to this file (`.` for auto-name)
`-Pause+`	Pause between tests (seconds, integer or float)
`-Plugins+`	List of plugins to run (default: ALL)
`-port+`	Port to use (default 80)
`-RSAcert+`	Client certificate file
`-root+`	Prepend root value to all requests, format is /directory
`-Save`	Save positive responses to this directory (`.` for auto-name)
`-ssl`	Force ssl mode on port
`-Tuning+`	1 Interesting File / Seen in logs 2 Misconfiguration / Default File 3 Information Disclosure 4 Injection (XSS/Script/HTML) 5 Remote File Retrieval - Inside Web Root 6 Denial of Service 7 Remote File Retrieval - Server Wide 8 Command Execution / Remote Shell 9 [SQL Injection](/penetration-testing/web-app/sql-injection/) 0 File Upload a Authentication Bypass b Software Identification c Remote Source Inclusion x Reverse Tuning Options (i.e., include all except specified)
`-timeout+`	Timeout for requests (default 10 seconds)

OPTION	VALUE
`-Userdbs`	Load only user databases, not the standard databases all Disable standard dbs and load only user dbs tests Disable only db_tests and load udb_tests
`-until`	Run until the specified time or duration
`-update`	Update databases and plugins from CIRT.net
`-useproxy`	Use the proxy defined in nikto.conf
`-Version`	Print plugin and database versions
`-vhost+`	Virtual host (for Host header)

Nikto Example Commands

Nikto Scanning

The following nikto commands allow you to run basic nikto scans against a web application.

COMMAND	DESCRIPTION
`nikto -h [target]`	Basic scan, no HTTP options.
`nikto -h [target] -Tuning [tuning]`	Scan with a specific tuning.
`nikto -h [target] -mutate [mutate]`	Scan with a specific mutation.
`nikto -h [target] -ssl`	Scan using SSL.
`nikto -h [target] -nointeractive`	Run the scan non-interactively.

Nikto Using a Proxy

Using Nikto with a proxy such as Burp or another intercepting proxy.

COMMAND	DESCRIPTION
`-useproxy`	Enable usage of the HTTP/SOCKS proxy
`-noproxy`	Specify comma separated list of hosts not to use proxy for
`-proxyhost`	Hostname or IP address of the HTTP/SOCKS proxy
`-proxyport`	Port of the HTTP/SOCKS proxy
`-proxypass`	Password for the HTTP/SOCKS proxy
`-proxyuser`	Username for the HTTP/SOCKS proxy

Nikto2 Features

- 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