NIKTO WEB APP SCANNER
Software Guide

cloud academy
A QA COMPANY

NIKTO WEB APP SCANNER

This guide covers the basics of using Nikto, the web app vulnerability scanner. Nikto is one of the most commonly used website vulnerability tools in penetration testing and is considered an industry standard tool.

Why use Nikto?

The main purpose of Nikto is to examine websites and webapps and report back to the tester with any vulnerabilities that can be implemented to hack or exploit the site.
This saves time in pen-testing and avoids having to manually find exploits for any found vulnerabilities.

Installing Nikto

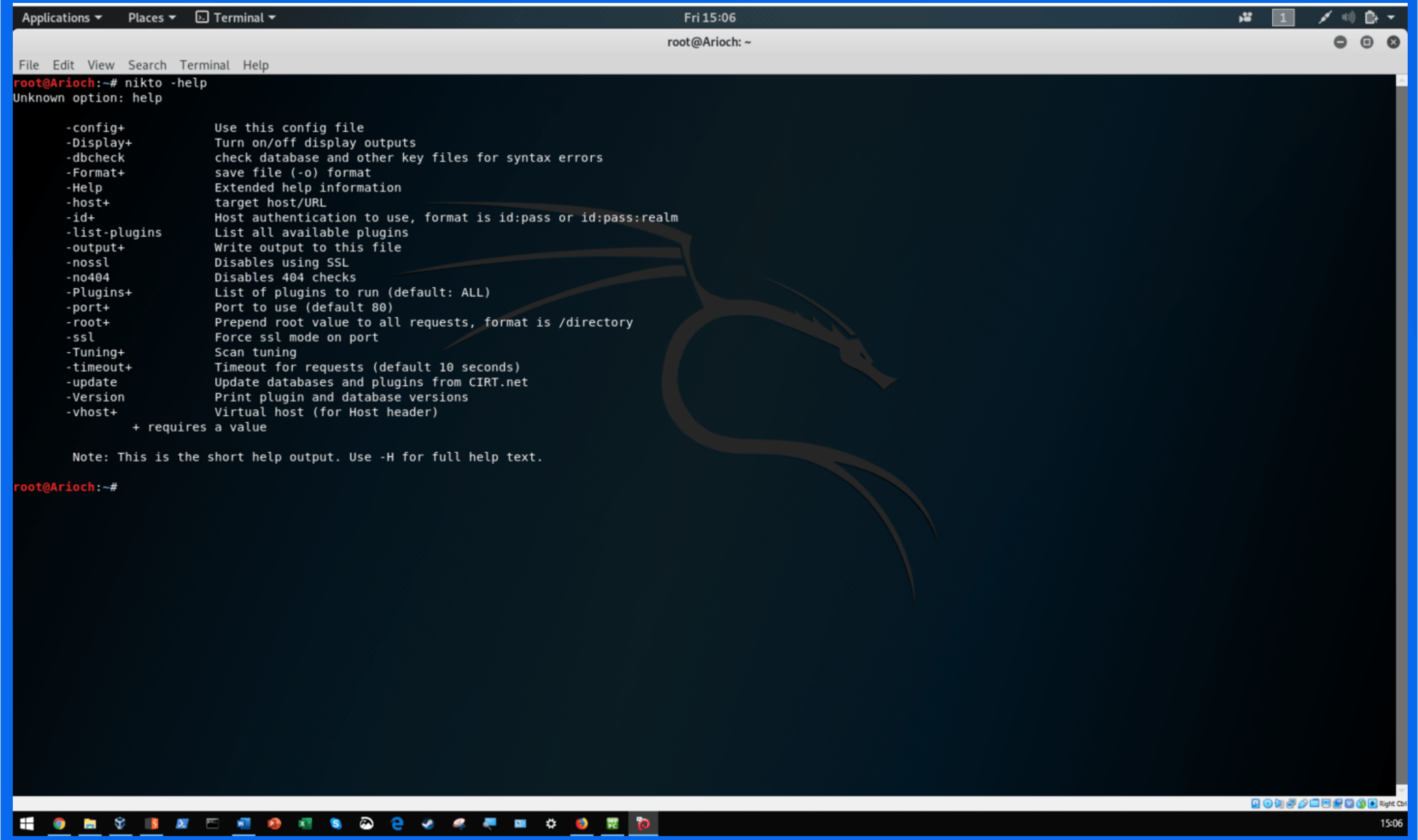
Nikto should be preinstalled on Kali Linux. If you need to install it, enter the following command in to the terminal:

```
apt-get install nikto
```

Get help in Nikto

If you require any help on what options to use in Nikto, you can use the below command to bring up the help screen. Enter *Clear* to remove it.

```
nikto -help
```



```
root@Arioch:~# nikto -help
Unknown option: help

       -config+            Use this config file
       -Display+           Turn on/off display outputs
       -dbcheck            check database and other key files for syntax errors
       -Format+            save file (-o) format
       -Help               Extended help information
       -host+              target host/URL
       -id+                Host authentication to use, format is id:pass or id:pass:realm
       -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 /directory
       -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@Arioch:~#
```

cloud academy
A QA COMPANY

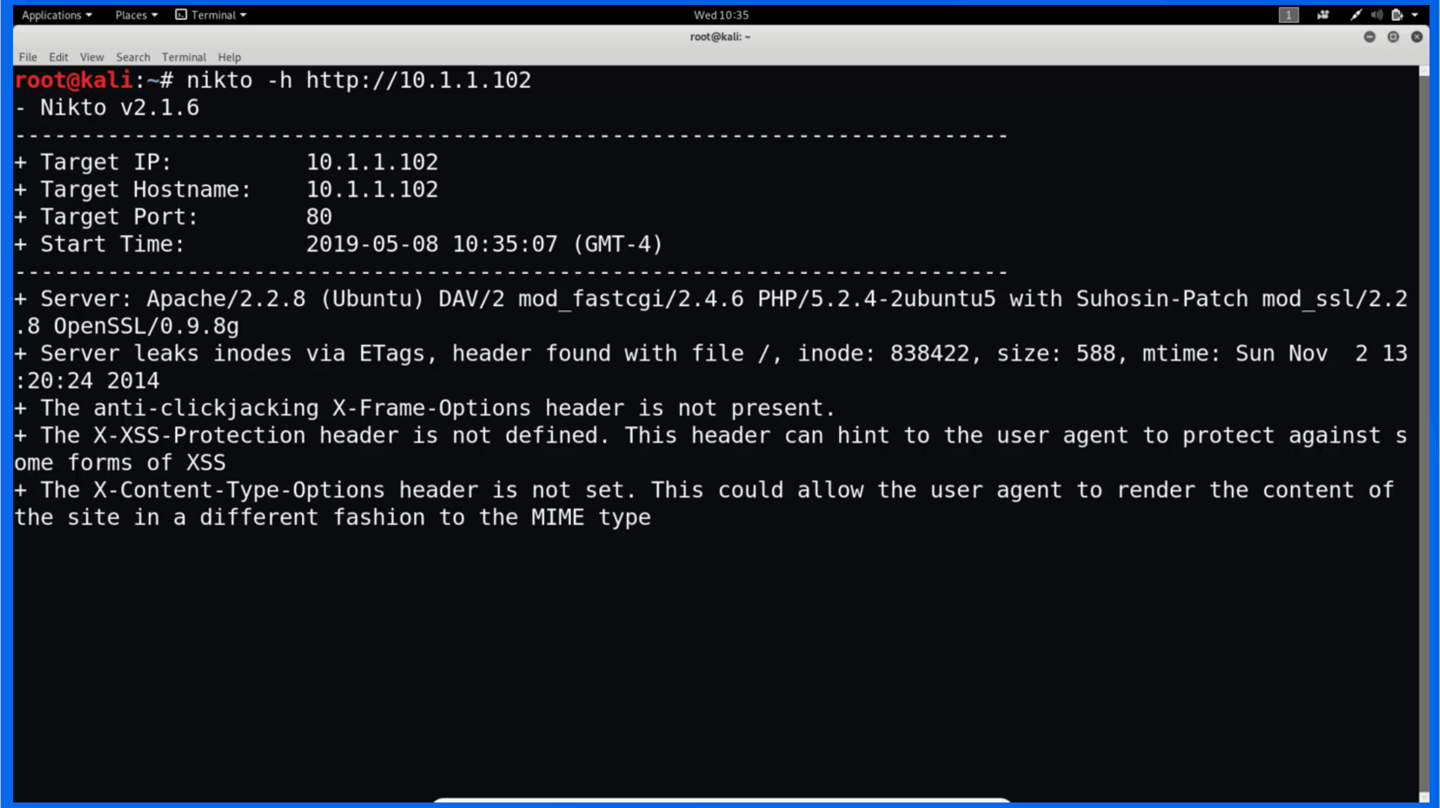
NIKTO WEB APP SCANNER

Scan an IP Address to find Vulnerabilities

Nikto should be used when you have already found a vulnerable IP address. Nikto will then scan the IP address and check these vulnerabilities against the Open Source Vulnerability Database, or OSVDB. Nikto can scan websites that are secured or unsecured using port 80 (HTTP) as well as SSL enabled sites.

In order to scan, you'll need to have your target IP address. Then, type the following command:

```
nikto -h [replace with IP address]
```



```
root@kali:~# nikto -h http://10.1.1.102
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.1.1.102
+ Target Hostname:    10.1.1.102
+ Target Port:        80
+ Start Time:         2019-05-08 10:35:07 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4-2ubuntu5 with Suhosin-Patch mod_ssl/2.2
.8 OpenSSL/0.9.8g
+ Server leaks inodes via ETags, header found with file /, inode: 838422, size: 588, mtime: Sun Nov  2 13
:20:24 2014
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against s
ome forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of
the site in a different fashion to the MIME type
```

Save Nikto Scan Output as HTML

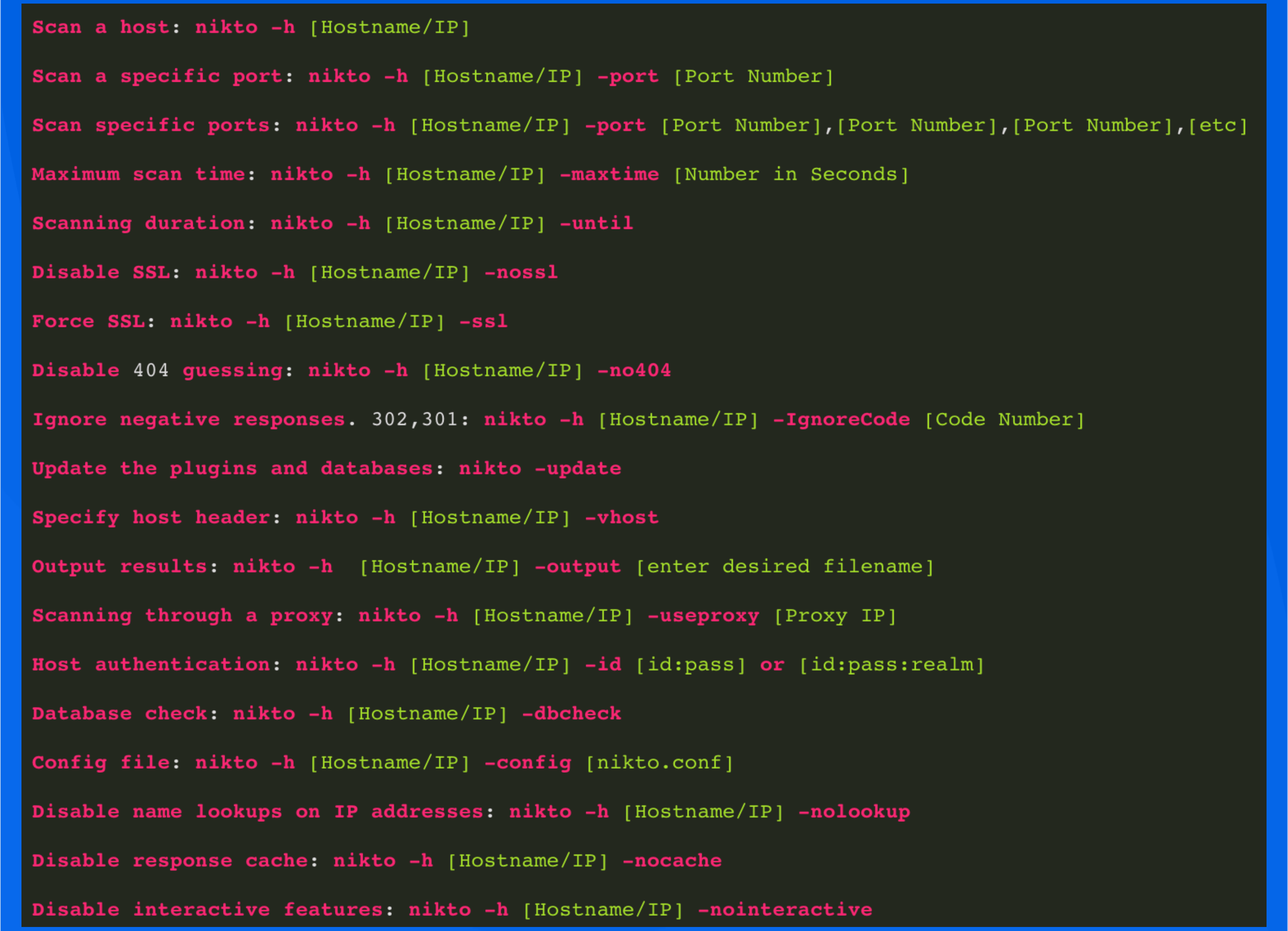
In order for the scan to be more human-readable, you can save the Nikto scan and its results as HTML, which can be read in any internet browser.
The page will show the associated OSVDB entries, as well as the known vulnerabilities that can be used.

The command to do so is:

```
nikto [Enter ip address or hostname here] -output
/root/Desktop/nikto_results -Format html.
```

NIKTO WEB APP SCANNER

Useful Nikto Commands



```
Scan a host: nikto -h [Hostname/IP]

Scan a specific port: nikto -h [Hostname/IP] -port [Port Number]

Scan specific ports: nikto -h [Hostname/IP] -port [Port Number],[Port Number],[Port Number],[etc]

Maximum scan time: nikto -h [Hostname/IP] -maxtime [Number in Seconds]

Scanning duration: nikto -h [Hostname/IP] -until

Disable SSL: nikto -h [Hostname/IP] -nossl

Force SSL: nikto -h [Hostname/IP] -ssl

Disable 404 guessing: nikto -h [Hostname/IP] -no404

Ignore negative responses. 302,301: nikto -h [Hostname/IP] -IgnoreCode [Code Number]

Update the plugins and databases: nikto -update

Specify host header: nikto -h [Hostname/IP] -vhost

Output results: nikto -h  [Hostname/IP] -output [enter desired filename]

Scanning through a proxy: nikto -h [Hostname/IP] -useproxy [Proxy IP]

Host authentication: nikto -h [Hostname/IP] -id [id:pass] or [id:pass:realm]

Database check: nikto -h [Hostname/IP] -dbcheck

Config file: nikto -h [Hostname/IP] -config [nikto.conf]

Disable name lookups on IP addresses: nikto -h [Hostname/IP] -nolookup

Disable response cache: nikto -h [Hostname/IP] -nocache

Disable interactive features: nikto -h [Hostname/IP] -nointeractive
```

cloud academy
A QA COMPANY