Websites are a critical part of almost every business or organization in the world. From your nearby florist to global brands, almost everyone uses a website as part of their branding.

Unfortunately, websites are also one of the most unsecured gateways through which an attacker can exploit your company.

Since most websites are not backed by strong technical teams, it is important to understand website and web application security to protect your organization.

Introducing Nikto

Nikto is an open source web server and web application scanner. Nikto can perform comprehensive tests against web servers for multiple security threats, including over 6700 potentially dangerous files/programs. Nikto can also perform checks for outdated web servers software, and version-specific problems.

Nikto was written and maintained by Sullo, CIRT, Inc. It is written in Perl and was originally released in late 2001.

It is currently maintained by David Lodge (you can find his blog here), though other contributors have been involved in the project as well.

Here are some of the cool things that Nikto can do:

- Find SQL injection, XSS, and other common vulnerabilities
- Identify installed software (via headers, favicons, and files)
- Guess subdomains
- Includes support for SSL (HTTPS) websites
- Saves reports in plain text, XML, HTML or CSV
- “Fish” for content on web servers

- Report unusual headers
- Check for server configuration items like multiple index files, HTTP server options, and so on
- Has full HTTP proxy support
- Guess credentials for authorization (including many default username/password combinations)
- Is configured with a template engine to easily customize reports
- Exports to Metasploit

How to Install Nikto

Since Nikto is a Perl-based program, it can run on most operating systems with the necessary Perl interpreter installed.

If you're using Kali Linux, Nikto comes preinstalled and will be present in the "Vulnerability Analysis" category.

If you don't have Nikto on Kali (for some reason), you can get Nikto from GitHub or just use the "apt install nikto" command.
For installing Nikto on Windows, you must first install the Perl interpreter. It can be downloaded from here: https://www.activestate.com/activeperl
For MacOS, you can use homebrew.

Complete installation instructions for all platforms can be found here.

How to Scan with Nikto

Now that you know what Nikto is and how to install it, let's go ahead and run some scans.

Warning:

Before we get into scanning, I want to emphasize that I am not responsible for any damage you do trying to attack systems.

Doing so is illegal.

You should have written permission before you ever try to scan a system or network.

Since Nikto is a command-line tool, you can use the help command to get a list of options:

```
> nikto -Help
```

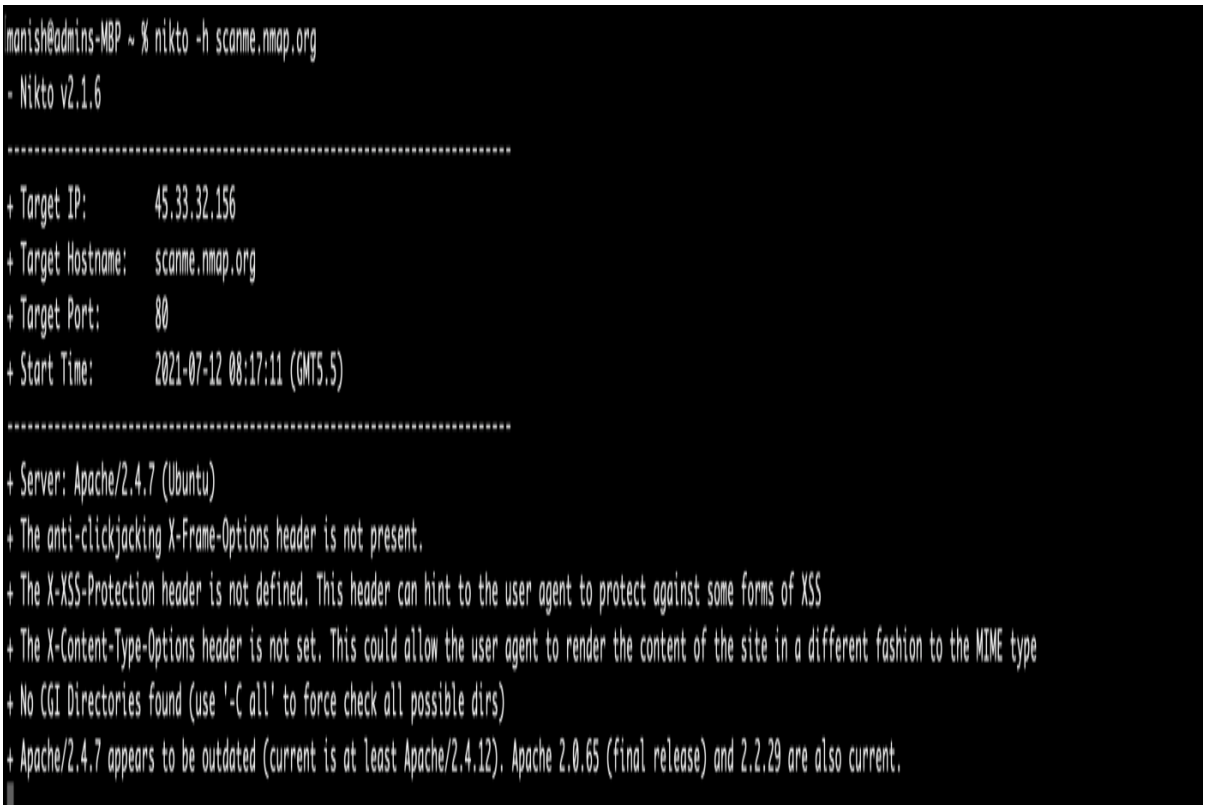
```
Options:
    -ask+               Whether to ask about submitting updates
                            yes   Ask about each (default)
                            no    Don't ask, don't send
                            auto  Don't ask, just send
    -Cgidirs+           Scan these CGI dirs: "none", "all", or values like "/cgi/ /cgi-a/"
    -config+            Use this config file
    -Display+           Turn on/off display outputs:
                            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+           Encoding technique:
                            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
                            B     Use binary value 0x0b as a request spacer
     -Format+           Save file (-o) format:
                            csv   Comma-separated-value
                            htm   HTML Format
                            nbe   Nessus NBE format
                            sql   Generic SQL (see docs for schema)
                            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
    -404code            Ignore these HTTP codes as negative responses (always). Format is "302,301".
    -404string          Ignore this string in response body content as negative response (always). Can be a regular expression.
    -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 (e.g., 1h, 60m, 3600s)
    -mutate+            Guess additional file names:
                            1     Test all files with all root directories
                            2     Guess for password file names
                            3     Enumerate user names via Apache (/~user type requests)
```

How to Scan a Domain

To perform a simple domain scan, use the `-h` (host) flag:

```
> nikto -h scanme.nmap.org
```

Nikto will perform a basic scan on port 80 for the given domain and give you a complete report based on the scans performed:



Nikto Domain Scan

How to Scan a Domain with SSL Enabled

For domains with HTTPS enabled, you have to specify the `-ssl` flag to scan port 443:

```
> nikto -h https://nmap.org -ssl
```

```
manish@admins-MBP ~ % nikto -h https://nmap.org --ssl
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          45.33.49.119
+ Target Hostname:    nmap.org
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=insecure.com
                   Altnames: insecure.com, insecure.org, issues.nmap.org, nmap.com, nmap.net, nmap.org, npcap.org, seclists.com, seclists.net, seclists.org, sectools.com, sectools.net,
sectools.org, secwiki.com, secwiki.net, secwiki.org, svn.nmap.org, www.nmap.org
                   Ciphers:  ECDHE-RSA-AES128-GCM-SHA256
                   Issuer:   /C=US/O=Let's Encrypt/CN=R3
+ Start Time:         2021-07-12 08:21:21 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.6 (CentOS)
+ 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 some 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
```

Nikto SSL Enabled Scan

How to Scan an IP Address

Sometimes you just want to scan an IP address where a web server is hosted.

To do that, use the same `-h` flag you used for domain scanning:

```
> nikto -h 45.33.32.156
```

```
manish@admins-MBP ~ % nikto -h 45.33.32.156
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          45.33.32.156
+ Target Hostname:    45.33.32.156
+ Target Port:        80
+ Start Time:         2021-07-12 08:24:14 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.7 (Ubuntu)
+ 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
+ The X-Content-Type-Options header is not set. This could allow the user agent to re
```

Nikto IP Address Scan

How to Scan Multiple IP Addresses From a Text File

To scan multiple IP addresses or domains, just put them in a text file separated by newlines. Nikto will know that the scan has to be performed on each domain / IP address.

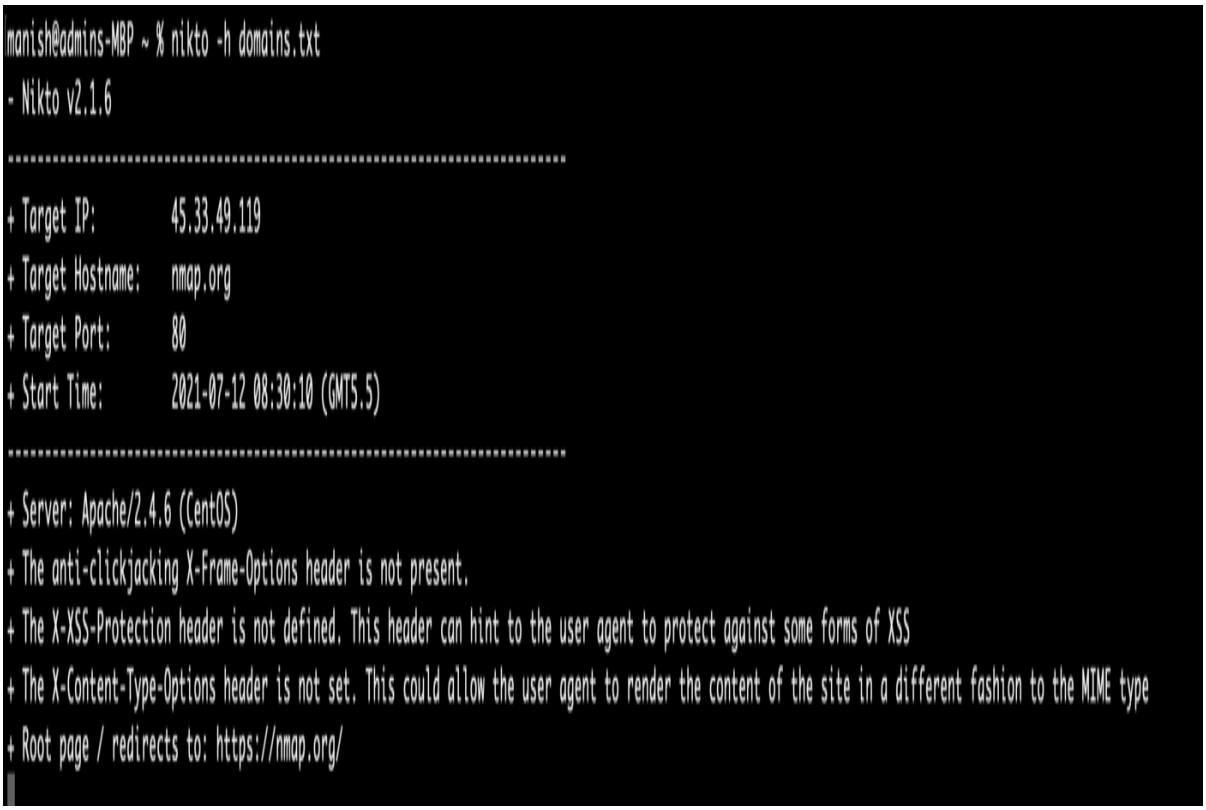
Let's assume we have a file named domains.txt with two domain names:

- scanme.nmap.org
- nmap.org.

To scan both of them with Nikto, run the following command:

```
> nikto -h domains.txt
```

Nikto will start scanning the domains one after the other:



Nikto Multi Domain Scan

How to Export Scan Results

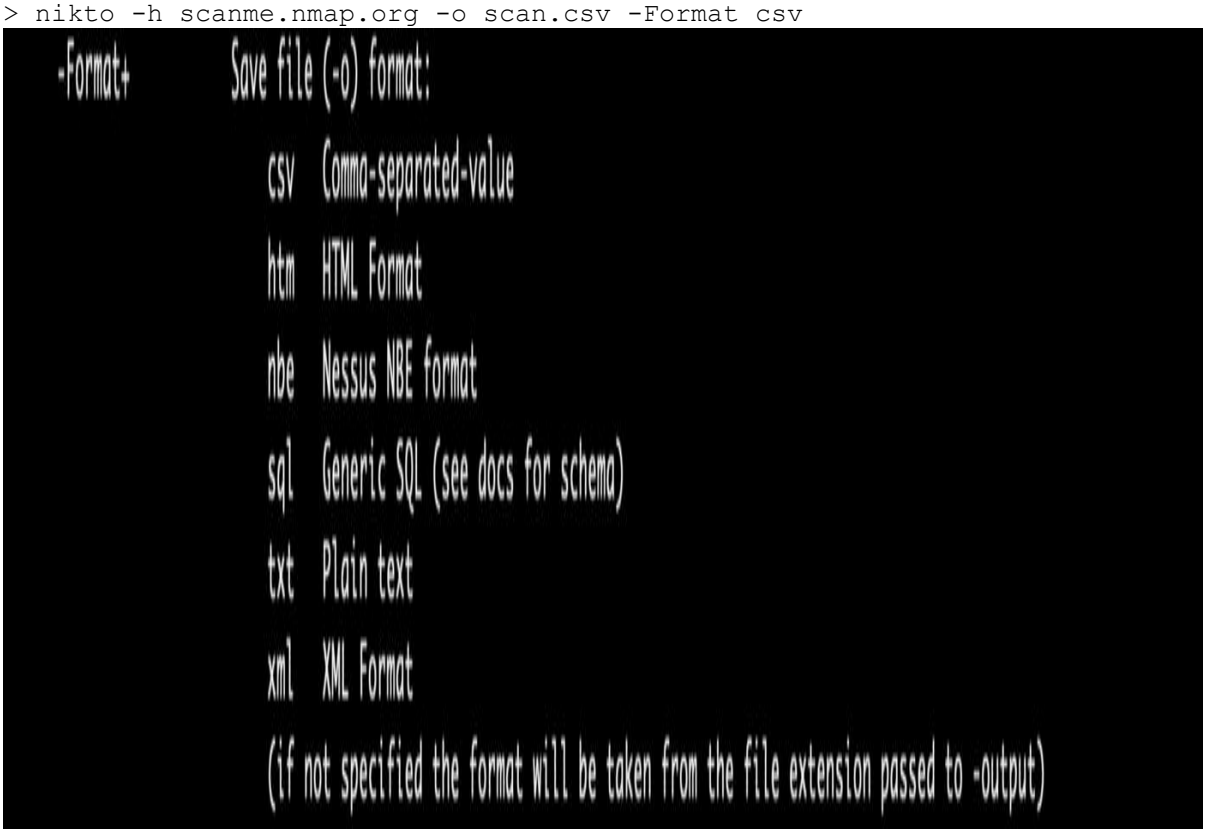
Nikto scans take a while to complete. When you are a professional pen-tester, you don't want to repeat scans very often unless there are major changes to the web application.

To export a scan result, use the `-o` flag followed by the file name:

```
> nikto -h scanme.nmap.org -o scan.txt
```

You can also use the `-Format` flag to specify an output format. You can choose from CSV, HTML, nbe (Nessus format), SQL, txt, and XML:

```
> nikto -h scanme.nmap.org -o scan.csv -Format csv
```



Nikto Output formats

How to Pair Nikto with Metasploit

Metasploit is a powerful framework that lets you do everything from scanning to exploiting systems. Professional pen-testers use Metasploit almost every day. I wrote a detailed article on Metasploit recently and you can find it here.

Nikto offers a way to export scans to Metasploit so that it gets easier when you try to exploit systems based on the scan results from Nikto.

To do that, append the `-Format msf+` flag to the end of a scan:

```
$ nikto -h <domain/ip> -Format msf+
```

Nikto Alternatives

It is always good to have a backup tool in your pen-testing arsenal. Some of the best Nikto alternatives are:

- **Arachni**: An open source, modular, high-performance Ruby framework with a focus on evaluating the security of web applications.
- **OWASP Zed Attack Proxy (ZAP)**: An integrated pen-testing tool that provides automated scanners as well as a set of tools that allow you to find security vulnerabilities manually.
- **Skipfish**: A fully automated, active web application security reconnaissance tool. Written in C to be fast, highly optimized HTTP handling, and minimal CPU footprint — easily achieving 2000 requests per second with responsive targets.

TLDR;

Nikto is an open source scanner that helps you find potential security threats in your websites and web applications.

It fully automates vulnerability scanning and can find issues like service misconfigurations, insecure files/programs, and thousands of other security issues.

Great alternatives include Arachini, OWASP ZAP, and Skipfish.

References

- https://cirt.net/Nikto2

- https://github.com/sullo/nikto
- https://linuxhint.com/scanning_vulnerabilities_nikto/
  Loved this article? ***Join my Newsletter*** *and get a summary of my articles and videos every Monday morning. You can also* ***visit my website here****.*