Nikto Website Scanner

Scan your web site and server immediately with the **popular Nikto Web Scanner.** This testing service can be used to test a Web Site, Virtual Host and Web Server for known security vulnerabilities and mis-configurations.

Nikto performs over 6000 tests against a website. The large number of tests for both security vulnerabilities and mis-configured web servers makes it a **go to tool for many security professionals and systems administrators**. It can find forgotten scripts and other hard to detect problems from an external perspective.

Testing Virtual Hosts with Nikto

If your web server hosts multiple sites using virtual hosts. You should test each virtual host using Nikto to get greater vulnerability coverage. In fact it can be helpful to scan the IP address as well as the hostname of the server to ensure all paths are tested for any vulnerable web applications and scripts.

Lengthy Nikto run time

Due to the number of security checks that this tool performs a scan can take **45 mins or even longer**, depending on the speed of your web server.

False Positives with Nikto

Nikto does quite well in detecting web server configurations that return HTTP 200 OK on actual "page not found" results. Since Nikto is checking hundreds of URL's for the presence of old scripts, vulnerable applications and other problems. This can sometimes result in many false positives if the detection of the 404 -> 200 is not discovered by Nikto. It is not difficult to spot as you will receive a

False Positives with Nikto

Nikto does quite well in detecting web server configurations that return HTTP 200 OK on actual “page not found” results. Since Nikto is checking hundreds of URL’s for the presence of old scripts, vulnerable applications and other problems. This can sometimes result in many false positives if the detection of the 404 -> 200 is not discovered by Nikto. It is not difficult to spot as you will receive a great deal of invalid urls as positives. These are easily checked manually to ensure they are actual false positives.

About the open source Nikto tool

The Nikto web server scanner is a security tool that will test a web site for thousands of possible security issues. Including dangerous files, mis-configured services, vulnerable scripts and other issues. It is open source and structured with plugins that extend the capabilities. These plugins are frequently updated with new security checks.

Nikto is by no means a stealthy tool. It will make over 2000 HTTP GET requests to the web server, creating a large number of entries in the web servers log files. This noise is actually an excellent way to test an in place Intrusion Detection System (IDS) that is in place. Any web server log monitoring, host based intrusion detection (HIDS) or network based intrusion detection (NIDS) should detect a Nikto scan.

Nikto Installation on Ubuntu

On a default installation of Ubuntu, launch a terminal and using a standard user account download the latest version of Nikto.

```
test@ubuntu:~$ wget
https://github.com/sullo/nikto/archi
ve/master.zip
```

You can unpack it with an archive manager tool or use tar and gzip together with this command.

```
test@ubuntu:~$ unzip master.zip
test@ubuntu:~$ cd nikto-
master/program
test@ubuntu:~/nikto-master/program$
perl nikto.pl
```

You should see the following output after running `nikto.pl` This should be your results from a working installation:

```
test@ubuntu:~/nikto-master/program$
perl nikto.pl
- Nikto v2.1.6
---------------------------------
---------------------------------
---
+ ERROR: No host or URL specified

       -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
```

Starting a Nikto Web Scan

For a simple test we will use test a single host name. In the example below we are testing the virtual host (nikto-test.com) on 16x.2xx.2xx.1xx over HTTPS. The web server on the target responds to the Nikto tests as it would any request to the web server, we can see from the results that the target is a WordPress based site.

```
test@ubuntu:~/nikto-master/program$
perl nikto.pl -host https://nikto-
test.com
- Nikto v2.1.6
---------------------------------
---------------------------------
---
+ Target IP:
16x.2xx.2xx.1xx
+ Target Hostname:    nikto-test.com
+ Target Port:        443
---------------------------------
---------------------------------
---
+ SSL Info:        Subject:
/CN=nikto-test.com
```

Nikto and the Web Server

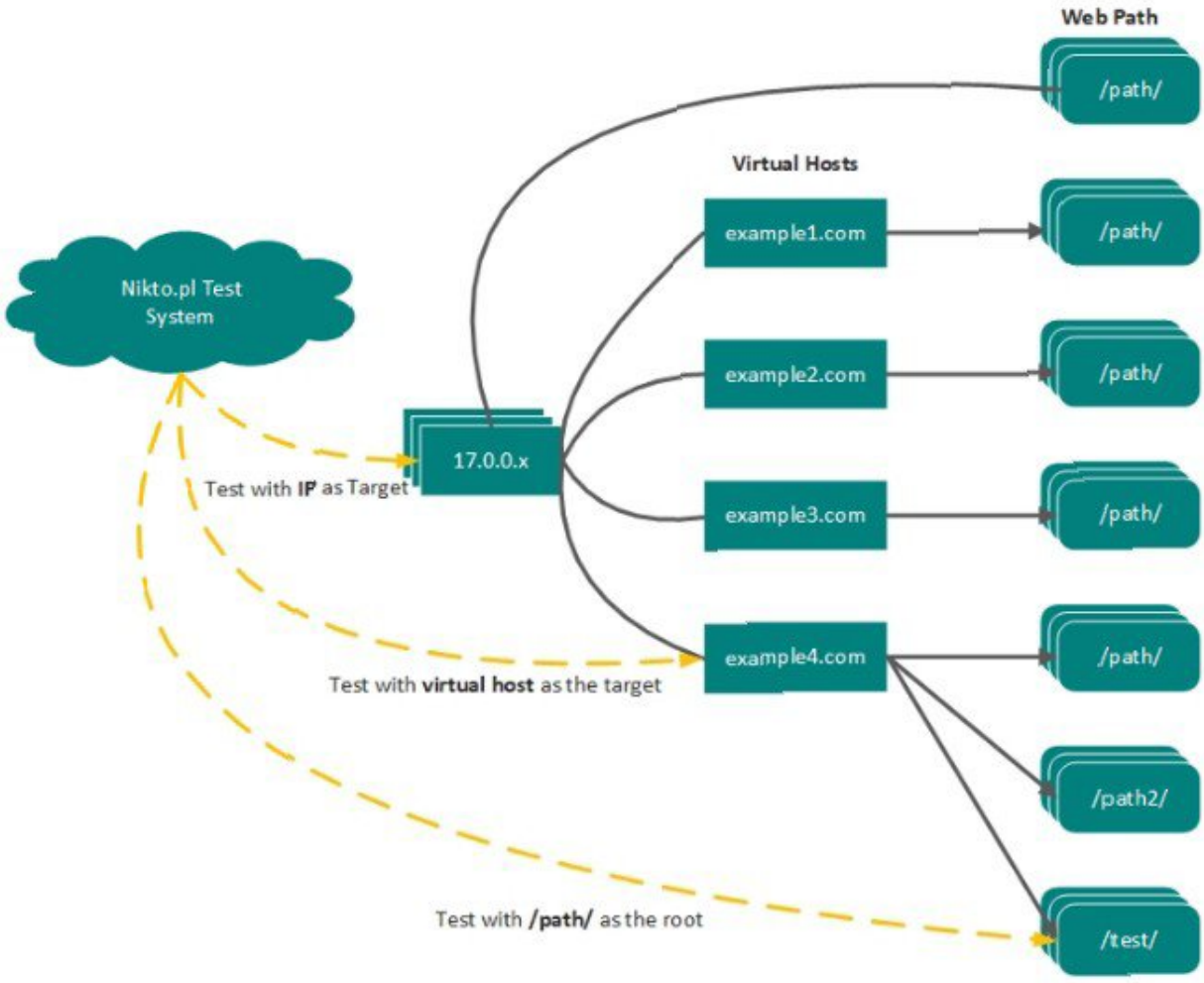
Lets review the web server logs. An important thing to understand when testing a site with Nikto is the amount of noise that this creates in the web server log files. Essentially Nikto is testing for the presence of thousands of possible web paths, and checking the response from the web server - which for most items will be a **404 not found**.

Here is a sample from an Nginx web server being tested by Nikto.

```
203.xxx.xxx.xxx - -
[25/Jun/2018:23:09:08 -0400] "GET
/iissamples/sdk/asp/docs/Winmsdp.exe
?
Source=/IISSAMPLES/%c0%ae%c0%ae/defa
ult.asp HTTP/1.1" 404 16611 "-"
"Mozilla/5.00 (Nikto/2.1.6)
(Evasions:None) (Test:003021)"
203.xxx.xxx.xxx - -
[25/Jun/2018:23:09:09 -0400] "GET
/iissamples/exair/howitworks/Winmsdp
.exe HTTP/1.1" 404 16611 "-"
```

Selecting the Target

Since the tool is checking for valid paths, it is important to remember that hitting a web server on different virtual host names, directly on the IP address and even on sub paths off the root of the site will give different results.



Lets take an example of PHPMyAdmin, this is a common tool for managing MySQL databases and can also be a good target for an attacker if it has not been patched or poorly managed. This

Conclusion

Nikto continues to be an excellent web server testing tool, finding all sorts of obscure issues whether its directory indexing, admin panels or remote code execution in a rare web application. Take the time to run it and be surprised.