Ethical Hacking Assignment 5

Web Hacking

(this assignment can be perform from home using your Kali Live USB)

First, let start my performing the following activities with Nitko:

Identify website vulnerabilities and attempt to exploit them using various tools. Perform SQL injection, web proxy, and Cross-Site Scripting (XSS) attacks. Tools: Nitko, WebScarp, OWASP-Zap and Social Engineering Toolkit (SET).

There are a number of tools and applications to find vulnerabilities in websites, but one of the simplest is nikto. This small and simple tool examines a website and reports back to you the potential vulnerabilities that it found that you could use to exploit or hack the site. In addition, it's one of the most widely used website vulnerabilities tools in the industry and in many circles considered the industry standard. Although this tool is extremely useful and effective, it is NOT stealthy. Any website with an [IDS](http://null-byte.wonderhowto.com/how-to/snort/) or other security measures in place will detect that you are scanning it. Originally designed for security testing, it was never meant to be stealthy.

<https://www.youtube.com/watch?v=IbENSVWq1wE>

<https://www.youtube.com/watch?v=aJN9bgFTysY>

Step 1: Fire Up Kali & Open Nikto

Let's fire up [Kali](http://null-byte.wonderhowto.com/how-to/hack-like-pro-getting-started-with-kali-your-new-hacking-system-0151631/) and get started with nikto. Once we have Kali up and running, go to Kali Linux -> Vulnerability Analysis -> Misc Scanners -> nikto, like in the screenshot below.[](http://img.wonderhowto.com/img/original/26/14/63530732481144/0/635307324811442614.jpg)

Although there are many options in using nikto, we will limit ourselves here to the basic syntax, such as this:

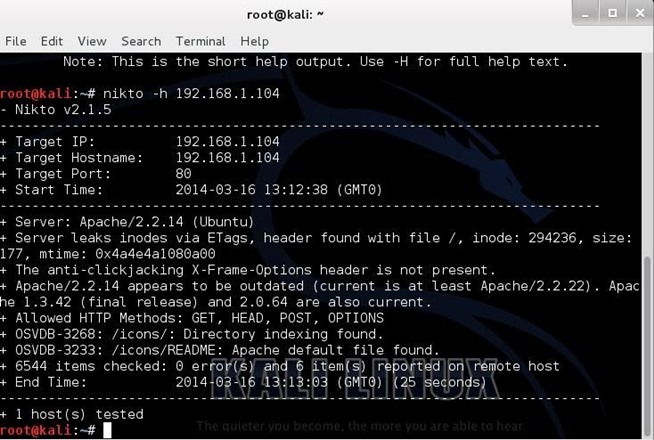
1. nikto -h <IP or hostname>

Step 2: Scan the Web Server Example

* nikto -h 192.168.1.104

Assume a web server is running on 192.168.1.104 in your internal network

Nikto responds with a lot of information, as you can see below.

[](http://img.wonderhowto.com/img/original/04/17/63530550948407/0/635305509484070417.jpg)

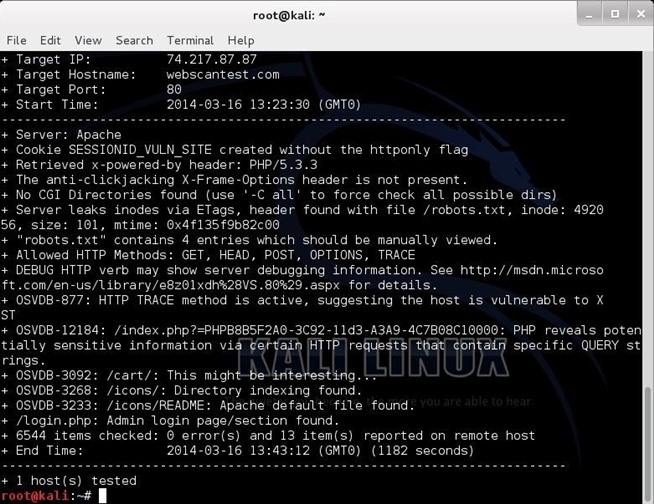
First, it tells us the server is Apache 2.2.14, probably on Ubuntu. It nailed this info and gives up more information on other potential vulnerabilities on this web server.

Note near the bottom that it identifies some vulnerability with the OSVDB prefix. This is the Open Source Vulnerability Database. This is a database maintained of known vulnerabilities at <http://cve.mitre.org/data/refs/refmap/source-OSVDB.html>

Step 3: Scan the Site

Let's try another site. There is a web server named webscantest.com that is made available to test various tools against, feel free to try it.. Let's see what nikto can tell us about this site.

* nikto -h webscantest.com or nikto –h testfire.net

[](http://img.wonderhowto.com/img/original/58/01/63530552809891/0/635305528098915801.jpg)

Once again, it identifies the server (Apache) and then proceeds to identify numerous potential vulnerabilities pre-fixed with OSVDB. We can take a look at that website at <http://cve.mitre.org/data/refs/refmap/source-OSVDB.html> to learn more about these vulnerabilities.

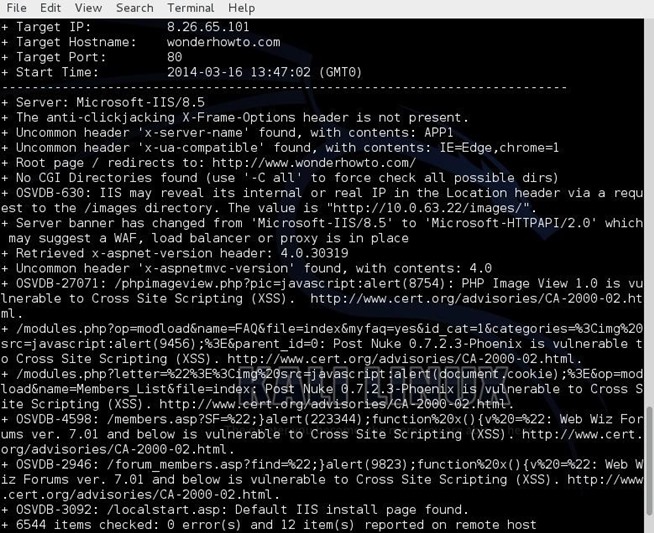
Now, let's use this site to find information on one of the vulnerabilities identified by nikto as OSVDB-877. We can put that reference number into [the search function](http://www.osvdb.org/search/web_vuln_search) and it retrieves [the following page](http://osvdb.org/877).

Note, in lower half of this page there are cross-references to the various information sources about this vulnerability, as well as references to tools and filters such as Nikto, Nessus, and [Snort](http://null-byte.wonderhowto.com/how-to/snort/).

Scan WonderHowTo

Let's scan a few more sites and see what it can tell us about these sites. Let's see what we can find out about then website, [www.wonderhowto.com](http://www.wonderhowto.com/).

* nikto -h wonderhowto.com

[](http://img.wonderhowto.com/img/original/73/16/63530553495344/0/635305534953447316.jpg)

As you can see, it tells us that WonderHowTo is using Microsoft's IIS 8.5 as a web server and then lists numerous potential vulnerabilities.

However, any attempt to exploit the vulnerabilities listed will reveal that they're all false-positives, as WonderHowTo simply returns a harmless 404 page. This is because WonderHowTo is not built on php or asp as the noted exploits expect.

False positives like this can appear because the scan does not actually execute each of the possible vulnerabilities, but rather scans to see if the server responds without error to known exploitable URLs.

1. Run nikto against testfire.net and indicate the three first CVEs associated with the OSVDB number, if available.

Only found two.

OSVDB-397: HTTP method (‘Allow’ Header): ‘PUT’ method could allow clients to save files on the web server.

OSVDB-5646: HTTP method (‘Allow’ Header): ‘DELETE’ may allow clients to remove files on the web server.

1. Run WebScrap, you must setup a proxy on your local machine’s web browser to intercept your website Request and Responds. See the following video for details <https://www.youtube.com/watch?v=VMyfDtkvPgU>

<https://www.youtube.com/watch?v=MhnhCuvEk8w>

Run a scan of the same website webtestscan.com. Did it perform the same functionality as the previous tools?

No. WebScarap sends requests and intercepts responses much like the man in the middle attack previously learned. It behaves like an intercepting proxy that allows the user to modify and review HTTP requests created by the browser before they get send to the server. It then displays both raw and parsed data.

What is the different between Lite and full-featured Modes?

The Lite and Full featured modes differ in what is provided. Lite mode provides you with the essential features of WebScarap while full featured mode displays all possible functions that are capable of being performed with WebScarap. Lite is also a subcategory of full feature.

What is an active and passive scan with respect to using this tool?

An active scan includes intercepting messages which means you actively went searching for information about messages sent back and forth using a man in the middle proxy. A passive scan will just intercept messages without looking for deep information.

1. OWASP-ZAP, visit the website owasp.org to learn more about this tool and other ones.

<https://www.youtube.com/watch?v=lJmfHmc4hxg>

<https://www.youtube.com/watch?v=_OxzY1_zE_U>

Please view these video and run the tool against the same website, once you have discovered the sites vulnerabilities, proceed to run the fuzzer to see if the site can be exploited, use these two video provide details on how to accomplish this.

<https://www.youtube.com/watch?v=cR4gw-cPZOA&index=7&list=PLEBitBW-Hlsv8cEIUntAO8st2UGhmrjUB>

<https://www.youtube.com/watch?v=5RmHyZkQo_8>

On what page did you run the fuzzer on? What is fuzzing? Which fuzzer was successful and on what field did you run it on?

I ran the fuzzer on testfire because that is what was showed to me in class and seemed like the most secure website made for doing things like this. Fuzzing is the act of inputting massive amounts of random data to the subject with the goal of causing a crash. If there is a weakness a fuzzer is used to identify the causes.

Of all of the tools, please write a short sentence describing what the tools do? Which tools do you please is the most effective and why?

WebScarap sends requests and intercepts responses much like a man in the middle attack.

OWASP ZAP can be used as a proxy server and permits the user to operate on the traffic that passes through it including https.

Nikto performs server type detailed checks and captures and prints any cookies received.

I think the best one is OWASP ZAP due to its easy GUI, multiple tools, and ease of learning.