Incomplete Lab - Web Vulnerability Scanning

Objectives

In this lab, you will complete the following objectives:

- Part 1: Launch Nikto and Perform a Basic Scan
- Part 2: Use Nikto to Scan Multiple Web Servers
- Part 3: Investigate Web Site Vulnerabilities
- Part 4: Export Nikto Results to a File

Background / Scenario

Nikto is a popular web vulnerability scanner that can find SQL injection, XSS, and other common vulnerabilities in websites. It can identify installed software using page headers and files. Nikto supports both HTTP and HTTPS protocols.

Required Resources

- Kali VM customized for the Ethical Hacker course
- Internet access

Instructions

Part 1: Launch Nikto and Perform a Basic Scan

Step 1: Launch Nikto on Kali Linux.

a. Log into the Kali system with the username **kali** and the password **kali**.
b. Nikto is preinstalled on Kali Linux. It is a command line tool that can be launched using the **Application -> Vulnerability Analysis -> nikto** choice on the menu, or directly from the command line. To view the help file, use the **nikto --help** command.

```
┌──(kali㉿Kali)-[~]
└─$ nikto --help
```

What command option will uncover SQL injection vulnerabilities only?

Answer Area

```
<!----><!---->
```

Step 2: Perform a basic scan on scanme.nmap.org.

a. Nmap.org has a website set up to test Nmap scans. You will use this web server to perform your first vulnerability scan. Launch Firefox and navigate to the **http://scanme.nmap.org** website. Read the description of the server and the restrictions that are placed on it.

What limitations does Nmap.org suggest for use of their server?

Answer Area

```
<!----><!---->
```

b. Use Nikto to perform a basic scan on the scanme.nmap.org website.

```
┌──(kali㉿Kali)-[~]
└─$ nikto -h scanme.nmap.org
```

Note: Nikto scans against an internet server can take a few minutes to complete. Wait until the CLI prompt is returned to continue to the next steps. To terminate a running scan, enter **CTRL-C**.

You should receive output similar to:

```
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Multiple IPs found: 45.33.32.156, 2600:3c01::f03c:91ff:fe18:bb2f
+ Target IP:          45.33.32.156
+ Target Hostname:    scanme.nmap.org
+ Target Port:        80
+ Start Time:         2023-05-23 05:48:36 (GMT-7)
---------------------------------------------------------------------------
```

```
+ Server: Apache/2.4.7 (Ubuntu)

+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

+ /: 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 M

+ No CGI Directories found (use '-C all' to force check all possible dirs)

+ /index: Uncommon header 'tcn' found, with contents: list.

+ /index: Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file names. The following alternatives for

+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.

+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response

+ Scan terminated: 20 error(s) and 5 item(s) reported on remote host

+ End Time:           2023-05-23 05:49:14 (GMT-7) (38 seconds)

---------------------------------------------------------------------------

+ 1 host(s) tested
```

c. Explore the link for **The X-Content-Type-Options header is not set.** vulnerability that was found. Open Firefox and navigate to the link: **https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/.**

d. Scroll down to view the summary, impact, remediation advice, and the associated vulnerability classification links.

What is the recommended remediation for this vulnerability?

Answer Area

<!----><!---->

e. Nikto scans for port 80 web services. To scan domains with HTTPS enabled, you must specify the **-ssl** flag to scan port 443:

```
┌──(kali㉿Kali)-[~]

└─$ nikto -h https://nmap.org -ssl
```

Part 2: Use Nikto to Scan Multiple Web Servers

In this part, you will use Nikto to scan servers on the internal virtual networks to look for vulnerable web servers. You will first create a text file to list the IP addresses that you want to scan. In real-life reconnaissance, you can obtain the IP addresses of the servers by doing a DNS lookup of the server name from the URL.

a. First, create a text file listing the IP addresses of the web servers to be scanned. Use the built-in MousePad application in Kali to create the file. Click **Applications ->Favorites->Text Editor**. Copy and paste this list of IP addresses into your document. Save the document to the home directory as **IP_list.txt**.

```
10.6.6.11

10.6.6.13

10.6.6.14

10.6.6.23

172.17.0.2
```

b. Run the scan using the **nikto -h IP_list.txt** command.

```
┌──(kali㉿Kali)-[~]

└─$ nikto -h IP_list.txt
```

Note: If you maximize the terminal window, the output will be easier to read.

How many of the targets are hosting web servers? How many servers are running Apache?

Answer Area

<!----><!---->

Part 3: Investigate Web Site Vulnerabilities

Nikto provides some information about the vulnerabilities that it uncovers during its scans. Some vulnerabilities are associated with an OSVDB number (an older Open Source Vulnerability Database), a CWE (Common Weakness Enumeration), or a CVE (Common Vulnerabilities and Exposures). OSVDB was discontinued in 2016. You can use the CVE reference tool to translate the OSVDB identifier to a CVE entry so you can research the vulnerability further.

a. Review the information that Nikto reported for the 172.17.0.2 web server. The CVEs listed in the output are CVE-1999-0678 and CVE-2003-1418. Use the CVE links in the Nikto output to find more information about the vulnerabilities.

What vulnerabilities are described by the two CVEs listed?

Answer Area

<!----><!---->

b. Use the National Vulnerability Database (https://nvd.nist.gov) to find additional information on the CVEs. In the References to Advisories, Solutions, and Tools section, follow the links to find the remediation measures needed to close each vulnerability.

What is the solution provided for CVE-2003-1418?

Answer Area

```
<!----><!---->
```

Part 4: Export Nikto Results to a File

Nikto can output the results of a scan in various formats including CSV, HTML, SQL, txt, and XML. In addition, Nikto can be paired with Metasploit to launch exploits against the vulnerabilities that you uncover.

a. To export a scan result, use the **-o** flag followed by the file name. Export the results of a scan to an HTML report file named **scan_results.htm**. The output file type is determined from the file extension.

```
┌──(kali㉿Kali)-[~]
└─$ nikto -h 172.17.0.2 -o scan_results.htm
```

b. Locate the file in the /home/kali directory and open it in your browser to view the report format.

c. To specify a text file output format that is independent of the file extension, use the **-Format** flag. Use the **-Format csv** option to save the file in .csv format to import into other analysis applications.

```
┌──(kali㉿Kali)-[~]
└─$ nikto -h 172.17.0.2 -o scan_results.txt -Format csv
```

d. Use the **cat** command to view the saved **scan_results.txt** file.

How does the saved file differ from the output shown on the screen?

Answer Area

```
<!----><!---->
```

Reflection

Nitko is an older open-source web vulnerability scanner. Use an internet search engine to search for other web vulnerability scanners that can be used with Kali Linux. List at least one additional tool that can be used to scan web sites for vulnerabilities that can be exploited.

Answer Area

```
<!----><!---->
```