Otis Smith

**Specialized Scanners (Core)**

**Learning Objectives:**

* Scan and enumerate web services on Windows.
* Research, download, and use specialized scanners based on results from scanning and enumeration tools.

1. Open Kali Linux.

Logged into Kali Linux by entering username “**kali**” and password “**kali**”

A screenshot of a computer

Description automatically generated

The **Kali VM machine** is now up.

A computer screen shot of a blue and white logo

Description automatically generated

1. Open Metasploitable 3 Windows Machine.

Powered up this **Metasploitable 3 Windows Machine** and clicked on the following order “**Input**”, “**Keyboard**”, **Insert Ctrl-alt-Del**” from the menu bar to get to the login screen.

A screenshot of a computer

Description automatically generated

Click on the **Administrator icon**.

A screenshot of a computer

Description automatically generated

1. Login to Metasploitable 3 as administrator and type "**start WampServer**" in the Windows search bar to ensure the service is running.

Enter the password “**vagrant**” hit “**enter**” or click the on blue arrow on the logon screen.

A screenshot of a computer

Description automatically generated

1. Click on the Start icon in the lower right corner, type in the command “**start WampServer**” to ensure the service is running which it is.

.

A screenshot of a computer

Description automatically generated

1. Minimize the **Metasploitable 3 Windows machine** and go back to **Kali Linux**.

Click the “**-**“symbol to minimize the **Metasploittable 3 Windows machine**

A screenshot of a computer

Description automatically generated

1. Perform a Nmap scan against the Metasploitable machine.

Move over to the **kali linux machine**, click on the new terminal “**Icon**” and enter in this command “**nmap 10.0.2.1-254**” to identify the IP address which provided the ip of “**10.0.2.9**” and perform the Nmap scan against the **Metasploitable machine**.

A screenshot of a computer program

Description automatically generated

Note: After the port scan was done, port **8585** did not show on the nmap scan.

Run the command “**nmap -p- 10.0.2.9**” to scan on all the ports to include port 8585 and other host. The port “**8585**” is listed as one of the ports.

A screenshot of a computer screen

Description automatically generated

1. Run a dirbuster scan against port 8585 as well as a Nikto scan.

Type in the command” **dirbuster**” and hit “**Enter**”

A screenshot of a computer

Description automatically generated

Use another way to open up “**dirbuster**” by clicking the blue kali icon from the top left corner. Enter “**dirbuster**” into the search field and double click on the result “**dirbuste**r”

A screenshot of a computer

Description automatically generated

Enter in <http://10.0.2.9:8585> in the Target URL field.

A screenshot of a computer

Description automatically generated

Click on Browse button, then select the dropdown arrow and on root “**/**” in the Look In: field.

A screenshot of a computer

Description automatically generated

Select “**usr**”

A screenshot of a computer

Description automatically generated

Select “**Share**”

A screenshot of a computer

Description automatically generated

Select “**wordlists**”

A screenshot of a computer

Description automatically generated

Select “**dirbuster**”

A screenshot of a computer

Description automatically generated

Select “**directory-list-2.3-medium.txt**” and click “**select List**” A screenshot of a computer

Description automatically generated

The scanning type path is **“/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt**” and enter**”.pdf, .doc, .docx, .ppt, .pptx, .pps, .ppsx, .odt, .xls, .xlsx, .PSD**” to the “**File extension**” field and then click “**Start**”

**Note: The list of wordpress file extension from a simple google search.**

A screenshot of a computer

Description automatically generated

The scan started.

A screenshot of a computer

Description automatically generated

As the scan ran on “**OWASP DirBuster**”, it simultaneously reflected the report on the “**kali screen**” of the found files.

A screenshot of a computer

Description automatically generatedkali

Stopped the after an hour of scanning, then clicked on “**Report**” to generate the report.

A screenshot of a computer

Description automatically generated

Selected the files **(.txt**) and (.**XML**) and then click on “**Browse**”

A screenshot of a computer

Description automatically generated

Selected “**Downloads**” and then click on “**Select Directory**”.

A screenshot of a computer

Description automatically generated

Click on “**Generate Report**”

A screenshot of a computer

Description automatically generated

Click “**Close**” after the report has been generated.

A screenshot of a computer

Description automatically generated

Went to the “**kali/Download**” and both files are listed. Did a “**cat**” command to display the report.

A screenshot of a computer

Description automatically generated

The **nikto software** is already installed on kali from the previous lab project assignment “**Web Assessment” so** moving forward.

Will install the **Nikto**.

Did a google search by inputting “**Nikto scanning tool** “and got to this page. Chose to go with “**Nikto: A Practical Website Vulnerability Scanner**”

A screenshot of a computer

Description automatically generated

This is web address” [**https://securitytrails.com/blog/nikto-website-vulnerability-scanner**](https://securitytrails.com/blog/nikto-website-vulnerability-scanner)”

A screenshot of a computer

Description automatically generated

Came across this part of the article “**Features Here are some of the major features of Nikto. See the**[**documentation**](https://github.com/sullo/nikto/wiki)**for a full list of features and how to use them**.”

A screenshot of a computer

Description automatically generated

Clicked on “**documentation**” provided this link “**https://github.com/sullo/nikto/wiki** “to get me to this page.

A screenshot of a computer

Description automatically generated

Back on the **Nikto** main page “[**https://securitytrails.com/blog/nikto-website-vulnerability-scanner**](https://securitytrails.com/blog/nikto-website-vulnerability-scanner)**”**

A screenshot of a website

Description automatically generated

Here are the provided instructions to install the Nikto tool on kali machine.

First, refresh your APT package lists and install any pending updates:

**sudo apt-get update && sudo apt-get upgrade**

**Next, install the Nikto web scanner with the command:**

**sudo apt-get install nikto -y**

**To verify that the Nikto website vulnerability scanner is installed and ready for use, run the command:**

**nikto**

**Which should then give you a similar output which lists the version of Nikto installed:**

**root@home:~# nikto**

**- Nikto v2.1.5**

A screenshot of a computer

Description automatically generated.

Logged onto to **kali** and opened a **new terminal**.

A screenshot of a computer

Description automatically generated

Use the command “**sudo apt-get update && sudo apt-get upgrade**” then hit “**Enter**”. Input the password “**kali**”

Note: always input the letter “**Y**” when prompted.

A screenshot of a computer

Description automatically generated

Now, the update and upgrade are done. Enter the command “**sudo apt-get install nikto -y**”

A screenshot of a computer

Description automatically generated

Received this error “**dpkg was interrupted, you must manually run 'sudo dpkg --configure -a' to correct the problem**.”

A screenshot of a computer

Description automatically generated

Decided to use the “**sudo dpkg --configure -a**” command and hit “**Enter**”.

A computer screen shot of a code

Description automatically generated

The “**dpkg—configure -a**” issue is now resolved.

A screen shot of a computer

Description automatically generated

Use this command “**sudo apt-get install nikto -y**” again.



The “**nikto**” is now installed.

A screen shot of a computer

Description automatically generated

Verify that the Nikto website vulnerability scanner is installed and ready for use by running this command “**nikto**”



The verification outcome:

A screenshot of a computer

Description automatically generated

Powered up both the” **Metasploitable 3 Windows machine**” machines.

Use the command “**nikto -h 10.0.2.9 -p 8585**” to scan port 8585 on the “**Metasploitable 3 Windows machine** “and below is the result with some vulnerability found.

A screen shot of a computer

Description automatically generated

**Wordpress**

“/wordpress/readme.html: This WordPress file reveals the installed version.

+ /wordpress/wp-links-opml.php: Cookie nf\_wp\_session created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies

+ /wordpress/wp-links-opml.php: This WordPress script reveals the installed version.

+ /wordpress/wp-login.php?action=register: Cookie wordpress\_test\_cookie created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies

+ /wordpress/wp-content/uploads/: Directory indexing found.

+ /wordpress/wp-content/uploads/: Wordpress uploads directory is browsable. This may reveal sensitive information.

+ /wordpress/wp-login.php: Wordpress login found.

+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.”

1. Research to find a specialized scanner for port 8585 and enumerate it.

Did a google search “**What specialized scanner to use for port 8585 scanning** “and the search return this page listed below:

A screenshot of a computer

Description automatically generated

Decided to use option tool number 4 call “**Netcat**”

A screenshot of a computer

Description automatically generated

Use the command “**ncat**” to install the software.

A screenshot of a computer program

Description automatically generated

Did the “**ncat –-help**” command to list the various option swithes available.

A screenshot of a computer screen

Description automatically generated

Use the command “**ncat 10.0.2.9 8585 -v**” and “**ls**” to exploit the target machine.

A screenshot of a computer program

Description automatically generated A screenshot of a computer screen

Description automatically generated A screenshot of a computer

Description automatically generated A screenshot of a computer program

Description automatically generated

Here are some of the findings from the outcome.

"http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd">

<title>WAMPSERVER Homepage</title>

<meta http-equiv="Content-Type" content="txt/html; charset=utf-8" />

background: url(index.php?img=pngPlugin) 2px 50% no-repeat;

<link rel="shortcut icon" href="index.php?img=favicon" type="image/ico" />

<h1><abbr title="Windows">W</abbr><abbr title="Apache">A</abbr><abbr title="MySQL">M</abbr><abbr title="PHP">P</abbr></h1>

<li><a href="http://www.wampserver.com">WampServer</a></li> -

<li><a href="http://www.wampserver.com/en/donations.php">Donate</a></li> -

<li><a href="http://www.alterway.fr">Alter Way</a></li> “

Use the command “**ncat 10.0.2.9 8585 -v**” to connect through the back door to exploit the machine.

A screen shot of a computer

Description automatically generated

1. Find the flag.

Use the nmap command “**nmap -p 8585 -T4 -A -v 10.0.2.9**” to find the flag.

A screenshot of a computer program

Description automatically generated

Fixes to Known Issues

**Is port 8585 not showing on your nmap scan?**

The solution to this is to scan ALL ports using the "-p-" switch

**Is port 8585 not showing EVEN AFTER you scan all ports with nmap?**

The solution is that you may have to log in to the Windows machine, log in as the administrator, and manually start WAMP. it will be "start WampServer" when you type it into the start menu.

**Mitigation and Outcomes:**

1. **Nmap Scan:**
   * *Observations:*
     + Successfully identified Metasploitable 3 Windows machine IP (10.0.2.9).
     + Discovered open ports using Nmap, revealing potential vulnerabilities.
   * *Mitigation:*
     + Addressed the issue of port 8585 not showing by scanning all ports with the "-p-" switch.
     + Provided a solution for cases where port 8585 doesn't appear even after an exhaustive scan.
2. **DirBuster and Nikto Scans:**
   * *Observations:*
     + Executed DirBuster scan on port 8585, revealing directories and files.
     + Conducted a Nikto scan, identifying vulnerabilities related to WordPress installations.
   * *Mitigation:*
     + DirBuster results highlighted potential information exposure and emphasized the importance of securing sensitive directories.
     + Nikto identified WordPress-related vulnerabilities, indicating the need for timely updates and security measures.
3. **Specialized Scanner (Netcat):**
   * *Observations:*
     + Used Netcat (ncat) to connect to port 8585, revealing the WAMPSERVER homepage.
     + Attempted further exploration through Netcat, providing insights into the machine's configuration.
   * *Mitigation:*
     + Highlighted the potential risks associated with open ports and recommended securing services and configurations.
     + Emphasized the importance of using specialized scanners like Netcat for in-depth analysis and exploitation.
4. **Finding the Flag:**
   * *Observations:*
     + Utilized Nmap to perform a targeted scan for the flag on port 8585.
   * *Mitigation:*
     + Demonstrated the use of Nmap for flag identification, emphasizing its versatility in network reconnaissance.
     + Encouraged users to troubleshoot common issues related to port visibility and service startup.

**Fixes to Known Issues:**

* Provided a solution for port 8585 not showing on Nmap scans by using the "-p-" switch.
* Addressed cases where port 8585 continued to be undetected, suggesting manual initiation of WAMP on the Windows machine.

The practical engagement with specialized scanners and comprehensive scanning tools demonstrates a thorough understanding of penetration testing methodologies. The mitigation strategies outlined aim to enhance security awareness and encourage proactive measures in response to identified vulnerabilities.