Linux Learning Centre

NIKTO & WPSCAN

Penetration Testing Tools

LLC 500 CYBERSECURITY AND ETHICAL HACKING

Linux Learning Centre Ltd
www.linuxlearningcentre.co.ke

Nikto

Nikto is a simple, open-source web server scanner that examines a website and reports back vulnerabilities that it found which could be used to exploit the site.

Although this tool is extremely effective, it's *not* stealthy at all. Any site with an intrusion-detection system or other security measures in place will detect that it's being scanned.

Using NIkto

Install Nikto:

```
apt install nikto
```

Use the basic syntax

```
nikto -h <IP or hostname>
```

If it's an SSL site

```
nikto -h <IP or hostname> -ssl
```

```
nikto -h linuxlearningcentre.co.ke -ssl
```

Using NIkto

Scan an IP Address:

Check your ip: **ifconfig**

Then we can run ipcalc on it to get our network range. If you don't have ipcalc, you can install it with apt install ipcalc, then try again.

```
ipcalc 192.168.0.48
```

Run Nmap to find services running in the network

```
nmap -p 80 192.168.0.0/24 -oG results.txt
```

Using NIkto

We use cat to read the output stored in our results.txt document (or whatever you named it). Then, there's awk, a Linux tool that will help search for the following pattern, where Up means the host is up and print $2 means to print out the second word in that line for each, i.e., just the IP address. Then, we send that data to a new file called targetIP.txt

```
cat results.txt | awk '/Up$/{print $2}' | cat >> targetIP.txt
```

We can now view the contents of our new file with cat to see all the IP addresses that have port 80 open.

```
cat targetIP.txt
```

Output

we can send this output over to Nikto with the following command.

nikto -h targetIP.txt

Scan a HTTP Website

nikto -h linuxlearningcentre.co.ke

WPSCAN

Nikto

This scanner tool scans for vulnerabilities in websites that run WordPress web engines.

- Checking the version of WordPress used and associated vulnerabilities for that version.
- Checks for database dumps that may be openly accessible.
- Checks for the WordPress README file.
- Brute force usernames and passwords if possible.
- Checks for publicly available or backed up wp-config.php files
- Checks for themes and plugins used on the site and possible vulnerabilities for them.
- Performs media file enumeration as well.
- Checks for exposed error log files, if available.
- Also, enumerates possible directory lists.

WPSCAN USAGE

Install Wpscan:

```
apt-get install wpscan
```

```
wpscan --url <https://recon_site.com>
```

WPSCAN Options

–url URL It is a mandatory argument that supplies the URL of the blog to be enumerated.

-o FILE saves the output to a given file.

-hh displays the full help

-detection-mode MODE sets the mode of enumeration. Available modes are:

1. mixed: performs a medium level of enumeration.
2. passive: scans only a few vulnerabilities
3. aggressive: performs deep rigorous scan of the website.

–force does not check if the URL supplied uses WordPress or not.

–api-token API without this option, wpscan does not display enumerated vulnerabilities.

Linux Learning Centre Ltd
www.linuxlearningcentre.co.ke