Walkthrough – VulnOS 2

Contents

[Host Discovery 2](#_Toc147659721)

[Nmap 2](#_Toc147659722)

[Services 3](#_Toc147659723)

[Nikto 3](#_Toc147659724)

[Dirb 3](#_Toc147659725)

[Viewing Website 3](#_Toc147659726)

[Wapiti 3](#_Toc147659727)

[FFuf 4](#_Toc147659728)

[Viewing Website 2 4](#_Toc147659729)

[Dirb 2 5](#_Toc147659730)

[DroopeScan 5](#_Toc147659731)

[Exploitation 5](#_Toc147659732)

[Upgrade Shell 6](#_Toc147659733)

[Finding Binaries 6](#_Toc147659734)

[Possible Accounts 6](#_Toc147659735)

[Linux Exploit Suggester (Les.sh) 7](#_Toc147659736)

[Flag 7](#_Toc147659737)

# Host Discovery

A black and white screen with white text

Description automatically generated

**Kali**: 192.168.56.101

**Victim**: 192.168.56.104

# Nmap



A black background with white text

Description automatically generated



A screenshot of a computer screen

Description automatically generated

# Services

OpenSSH 6.6.1 – This doesn’t have an exploit for this version, only 6.6.

Apache httpd 2.4.7 – There is a vulnerability that is a race condition.

Ngircd – There is an exploit, script 784. Script connects and creates shell.

# Nikto



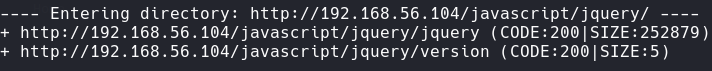
Nothing of interest is revealed.

# Dirb



A screenshot of a computer

Description automatically generated



# Viewing Website



The main website contains another link that leads to another url. This url is a company.



When clicking on each menu item on menu bar this url changes the last digit. This could be vulnerable.



This is a directory listing, and shows images, javascript, css.

# Wapiti



Wapiti states that there could be a vulnerability when modifying the url’s ‘q’ value.

# FFuf

The following were found to be viable:

1. Blog
2. 0
3. User
4. Node
5. Book
6. Cart
7. Tracker

These are not allowed but interesting: admin, checkout, aggregator, contact, search, batch

# Viewing Website 2

This states webmins blog.

Default webpage.



Login page found.

This gives access denied. So does 0. There must be two users (1 & 0).

This shows a blank table.

A screen shot of a computer

Description automatically generatedA screenshot of a computer screen

Description automatically generatedUser ‘1’ is not a proper username. So there might be another way to get in.



# Dirb 2



A screen shot of a computer code

Description automatically generated

# DroopeScan

A screenshot of a computer

Description automatically generated



I also ran nikto again and found drupal 7 was the framework.

# Exploitation

A screen shot of a computer

Description automatically generatedKnow that drupal 7 is being used I could then use searchsploit to see any form of vulnerability. I did see remote code execution and I saw a php file to use. However I didn’t know where to begin so I had to use msfconsole instead.

The one highlighted is what searchsploit had, so I will use this in msfconsole.

A screen shot of a computer

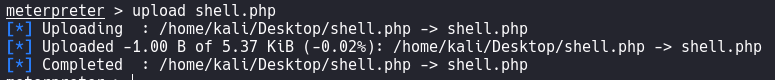
Description automatically generated

I did the following changes.

A screenshot of a computer

Description automatically generatedI changed the target URI because the drupal website is actually in the <http://192.168.56.104/jabc>.

Now I am in the server.

For the sake of not using too much msfconsole I will only use it to upload the shell.php file that I have.

A computer screen with white text

Description automatically generatedReverse shell is now up.

## Upgrade Shell



## Finding Binaries

A screen shot of a computer

Description automatically generated

## Possible Accounts

This could be a possible account that I need to get the password of.

## Linux Exploit Suggester (Les.sh)

A screenshot of a computer

Description automatically generatedThe script that I downloaded from my http python server using the wget command in the victims temp directory suggests that dirtycow and dirty cow 2 is a vulnerability. However it also shows an exploit called overlayfs is an exploit.

I downloaded the exploit given the link provided and downloaded it using wget from my python server.



Compiled it.



A screen shot of a computer

Description automatically generatedBefore

After

# Flag

A black background with white text

Description automatically generatedThe flag is located in the root directory.

**NOTE**: This is the first VulnHub I did by myself without any walkthrough. Only exploitDB, and google searches for exploits. I did finished at from 10:00 - 11:46am 25/09/2023.