Walkthrough - VulnOS

Contents

[Host Discovery 2](#_Toc147659864)

[Nmap 2](#_Toc147659865)

[Nikto 2](#_Toc147659866)

[Dirb 2](#_Toc147659867)

[Viewing Website 3](#_Toc147659868)

[Exploitation 3](#_Toc147659869)

[Msfconsole 3](#_Toc147659870)

[SSH 4](#_Toc147659871)

[Escalation 5](#_Toc147659872)

[Flag 5](#_Toc147659873)

# Host Discovery

A black and white screen with white text

Description automatically generated

**Kali**: 192.168.56.101.

**Victim**: 192.168.56.146.

# Nmap

A computer screen shot of a program

Description automatically generatedA screenshot of a computer program

Description automatically generated

# Nikto



These were found, so I will investigate these.

# Dirb



A screen shot of a computer code

Description automatically generated

A screen shot of a computer code

Description automatically generated



PhpPGAdmin – PostGreSQL.

# Viewing Website

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

This is known to have a vulnerability for sql injection.

I couldn’t find much else and after using SQLMap on the login pages I couldn’t get any info. I went back to the ports open and found two interesting ones. Port 10,000 and 3632. The service on port 3632 is known to have a vulnerability that Metasploit has available. Port 10000 is a login page.

However I found on google that MiniServ 0.01 can reveal sensitive data. So I will check Metasploit.

# Exploitation

## Msfconsole





This is going to be the file that will be tested.

A black background with white text

Description automatically generated

A screen shot of a computer

Description automatically generatedNow that it works, I can pass in the file I found.

I don’t know why ldap.secret is used.

Password = canuhackme

For these possible accounts.



**HASH**:

$6$SLXu95CH$pVAdp447R4MEFKtHrWcDV7WIBuiP2Yp0NJTVPyg37K9U11SFuLena8p.xbnSVJFAeg1WO28ljNAPrlXaghLmo/

This has is SHA-512.

## SSH

The purple bit I had to include because I was getting and error that the key algorithms I was using wasn’t inline with the ssh server.

Credentials – vulnosadmin:canuhackme

Now that I am inside the linux machine I can download the les.sh script (which shows you exploits) and can see where to begin.

A computer screen shot of a computer code

Description automatically generatedAfter setting up a python server and downloading it into the tmp directory, I gave it execution privileges and ran ./les.sh

It is vulnerable to dirty cow 2.

A screen shot of a computer

Description automatically generated

# Escalation



Now that I have transferred the dirty cow 2 exploit to the victim I can then compile it with the above gcc parameters.

A screen shot of a computer screen

Description automatically generated

After running it a new account is made with root shell.



# Flag

A black background with white text

Description automatically generated