**VulnHub – Double Trouble 1 Walkthrough**

Contents

[Host Discovery 2](#_Toc145451038)

[Nmap 2](#_Toc145451039)

[Nikto 3](#_Toc145451040)

[Visiting Website 3](#_Toc145451041)

[StegHide 4](#_Toc145451042)

[StegSeek 4](#_Toc145451043)

[Exploiting 5](#_Toc145451044)

[Upgrade Shell 5](#_Toc145451045)

[Machine 2 6](#_Toc145451046)

[SQLMap 6](#_Toc145451047)

[SSH 7](#_Toc145451048)

[Flag 1 7](#_Toc145451049)

[Flag 2 7](#_Toc145451050)

# Host Discovery

A black and white screen with white text

Description automatically generatedOur IP: 192.168.56.101/24 (obtained using “ip a”).

Victim Machine: 192.168.56.131/24.

# Nmap

A black background with white text

Description automatically generated

Now repeat the above command and look for the version and service of the ports.



# Nikto

A screenshot of a computer screen

Description automatically generated

With some of the results, it might be worth using dirb, gobuster or some other directory enumeration tool.

# A screenshot of a login box Description automatically generatedVisiting Website



Viewing the website reveals that the default <http://192.168.56.131> is a login page. The framework used is qdPM 9.1.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

Starting from secret, I realised that you could store code in images and even other files. This is called steganography. I installed StegSeek to help me get into this file.

# StegHide



This asked me for a password to unlock this file and retrieve the contents. I don’t know it so I had to move onto another piece of software.

# StegSeek



A screenshot of a computer

Description automatically generated

This is the quickest software that is available.



These are the retrieved credentials, to login to the website.

# Exploiting

A screenshot of a computer

Description automatically generatedOn the dashboard navigate to the users tab and add a new user. Since the photo section doesn’t validate the input, we can upload our ‘pentestmonkey-reverse-shell’ script onto the site. Once we do this we can open a new terminal and run a netcat listen command on the same port used in the reverse shell.

A screenshot of a computer

Description automatically generated

Then navigate to the uploads index and click shell.php. Netcat will establish a connection if completed properly.

## Upgrade Shell

A computer screen with white text

Description automatically generated

Running the ‘sudo –l’ command I can see I can run awk without a password.

On GTFO Bins it says if you can run this command as sudo then you can escalate privilege.

A close up of a black background

Description automatically generated

I now have root access.





There is no root flag. Instead we have another OVA file to install.

# Machine 2

The IP for the new machine is: 192.168.56.132/24. The same ports are open.

A screenshot of a login box

Description automatically generated

The website shows what appears to be an admin login page for maybe a database.

SQLMap will be used to leak information.

# SQLMap

A black background with white text

Description automatically generatedI got the below information from just running the sqlmap from the start menu and entering the url.







A screen shot of a computer

Description automatically generatedResults

# SSH





# Flag 1

I found the first flag file.



# Flag 2

Finding this requires a kernel level exploit.

Then google it, you should see an exploit available on exploit-DB (in this case 40839).

Compile it with the above flags.

Run it with root as an arg.





A computer code with white text

Description automatically generated

A close up of white text

Description automatically generated

Cat the flag, using ‘cat root.txt’.

