**Walkthrough – NullByte 1**

Contents

[Host Discovery 2](#_Toc146051168)

[Nmap 2](#_Toc146051169)

[Nikto 2](#_Toc146051170)

[Dirb 3](#_Toc146051171)

[Exiftool 3](#_Toc146051172)

[Viewing Website 3](#_Toc146051173)

[Hydra 3](#_Toc146051174)

[SQLMap 3](#_Toc146051175)

[Hashes.com 5](#_Toc146051176)

[SSH 5](#_Toc146051177)

[Exploitation 5](#_Toc146051178)

[Searching for Binaries 5](#_Toc146051179)

[Flag 6](#_Toc146051180)

# Host Discovery

A black background with white text

Description automatically generated

**Victim**: 192.168.56.139/24

**Kali**: 192.168.56.101/24

# Nmap



A black background with white text

Description automatically generated

A black background with white text

Description automatically generated

# Nikto





# Dirb

A screen shot of a computer

Description automatically generated

# Exiftool

Looking at the image you can download it. I will also used this tool to determine if the meta data contains anything important.



P-): kzMb5nVYJw

# Viewing Website

Secret Directory

Login Page for Database.

Default

Viewing the Secret Directory source code I can see this hint.

# Hydra

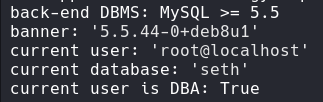
hydra -l none -P /usr/share/wordlists/rockyou.txt 192.168.56.139 http-post-form "/kzMb5nVYJw/index.php:key=^PASS^:invalid key"

I got ‘key’ attributed from the source code of website and I got index.php from incorrectly typing in the key.

# SQLMap

**URL**: <http://192.168.56.139/kzMb5nVYJw/420search.php?usrtosearch=a>

Once I got the key, I then proceeded to type a random search value ‘a’ and look at the url. I then then read the message that stated it was ‘fetching data’. This is an indicator that databases are at work.





A screen shot of a computer code

Description automatically generated

A screenshot of a computer program

Description automatically generatedThis command will retrieve the data from the database mysql and from table user.



A screenshot of a computer code

Description automatically generatedThen to make the data readable I used the above command.

**Credential Information**:

PhpMyAdmin: sunnyvale

A black background with white lines

Description automatically generatedRoot: Sunnyvale



**Hash**: YzZkNmJkN2ViZjgwNmY0M2M3NmFjYzM2ODE3MDNiODE

# Hashes.com



A green rectangle with numbers

Description automatically generated

After doing it twice, I found the hash value for the account Ramses: omega

# SSH





Given the credentials ramses:omega I was able to get into the ssh service on port 777.

# Exploitation

A black background with white text

Description automatically generatedI begin my checking if I can sudo on behalf of someone or without a password.

## Searching for Binaries

A black background with white text

Description automatically generatedI then looked for the possible binaries. I found poolkit.

https://www.exploit-db.com/exploits/50689

I created the ‘c’ files and then created a python server.

A screen shot of a computer

Description automatically generated

After they were downloaded in the victim’s /tmp directory I went to work giving the makefile execution privileges.



Then calling make.

A black background with white text

Description automatically generated

A black background with white text

Description automatically generatedOnce the code ran, the binary was ready.

A screenshot of a computer program

Description automatically generatedA close up of white text

Description automatically generatedThen executed ‘./exploit’.

I am now root.

# Flag

In the root directory I was able to get the flag called ‘proof.txt’.