**Walkthrough - School**

Contents

[Host Discovery 2](#_Toc145595617)

[Nmap 2](#_Toc145595618)

[Nikto 2](#_Toc145595619)

[Dirb 3](#_Toc145595620)

[Sub-dir found 3](#_Toc145595621)

[SQL File Analysis 3](#_Toc145595622)

[CrackStation 4](#_Toc145595623)

[Viewing Website 4](#_Toc145595624)

[Exploitation 4](#_Toc145595625)

[Upgrading Shell 5](#_Toc145595626)

[Finding binaries 6](#_Toc145595627)

[Root Directory 6](#_Toc145595628)

[MYSQL 7](#_Toc145595629)

# Host Discovery

**Kali Machine**: 192.168.56.101/24.

A black and white screen with white text

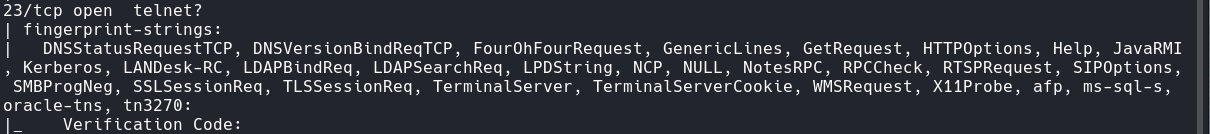
Description automatically generated

**Victim**: 192.168.56.136/24.

# Nmap



I tried an aggressive approach with this one, however this means I can easily be discovered.



A black background with white text

Description automatically generated

# Nikto





There are the interesting items found by nikto.

# Dirb





This database directory was found.

## Sub-dir found



# SQL File Analysis

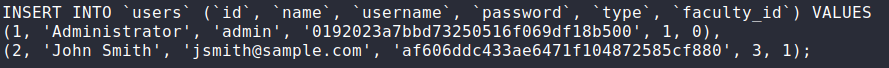
Downloading and opening the file shows table creation and data insertion.

A screenshot of a computer

Description automatically generatedGot some server information

Table Information





Found some valuable information.

(1, 'Administrator', 'admin', '0192023a7bbd73250516f069df18b500', 1, 0),

(2, 'John Smith', 'jsmith@sample.com', 'af606ddc433ae6471f104872585cf880', 3, 1);

Students:

(1, '06232014', 2, 'Claire Blake', '2020-10-28 11:53:24'),

(2, '123456', 2, 'George Wilson', '2020-10-28 15:20:57');

# CrackStation

Now its time to crack the hashes. I will use crackstation to decode and hash-identifier to determine the hash.



Admin

John

The admin credentials allow me to login to the student login page.

# Viewing Website

A screenshot of a login screen

Description automatically generated

Enter the credentials here.



A close-up of a white background

Description automatically generated

# Exploitation

Since we are greeted with the welcome back admin page, we can inspect the source code to see anything unusual or hints.

This is a very interesting line. I will take the href link. (‘index.php?page=site\_settings’)

A screenshot of a computer

Description automatically generated

A screenshot of a contact form

Description automatically generatedNow this allows a file to be uploaded.

I quickly set up a netcat:

Once I filled out the form, I then uploaded pentest monkeys reverse\_shell.php with the port 9999 and address of my kali machine.

A black background with white text

Description automatically generated

## Upgrading Shell



Looking through the home directory I see two directories.

Going into fox reveals a text file: local.txt.

I believe this may be the first flag. (*e4ed03b4852906b6cb716fc6ce0f9fd5*)

## Finding binaries

A computer screen shot of white text

Description automatically generated

# Root Directory

A black background with white text

Description automatically generated

There is the flag and a win binary.

A computer screen with white text

Description automatically generated

Since strings wasn’t found command, I used cat and found this.

I don’t know if its important, but I’ll keep looking. Next I ‘ll go to /var/www/html/student…/.

There are many php files listed.

A screen shot of a computer program

Description automatically generated

There is a file here called ‘db\_connect’ which sounds interesting.

$conn= new mysqli('localhost','fox','trallalleropititumpa','student\_attendance\_db')

This appears to be credentials for the database student\_attendance.

# MYSQL

A screen shot of a computer code

Description automatically generated

LEFT INCOMPLETE – ITS ADVANCED!