Walkthrough – Basic Pen Testing 1

Contents

[Host Discovery 2](#_Toc146544041)

# Host Discovery



# Nmap



# Nikto





In the secret directory found, I checked the source code and found this.

This means I need to change the hosts file to include ‘vtcsec’.

# Dirb



# Viewing Website

A screenshot of a login box

Description automatically generated

The credentials I guessed were admin:admin

# Exploitation

In the admin dashboard I went to the upload panel and uploaded the shell as a plugin.

A screenshot of a computer

Description automatically generatedThen I went to this url.

A screen shot of a computer

Description automatically generatedBefore submitting the url, I set up a netcat listener to listen on the same port (9999).

After upgrading shell, I am ready to begin escalation.

# Escalation

I found that /etc/passwd is writeable. So I decided to append a root line to this file so I can login as root.

A screen shot of a computer

Description automatically generatedPassword is toor.

I then opened it up, and added this.

Now I can switch user to toor (root user).

A black background with white text

Description automatically generated

Now I am root.