Walkthrough – Hackable II

Contents

[Host Discovery 2](#_Toc147356107)

[Nmap 2](#_Toc147356108)

[Viewing Website 2](#_Toc147356109)

[Nikto 3](#_Toc147356110)

[Dirb 3](#_Toc147356111)

[Exploitation 3](#_Toc147356112)

[Escalation 3](#_Toc147356113)

[Upgrade Shell 3](#_Toc147356114)

[Finding binaries 4](#_Toc147356115)

[Finding the file 4](#_Toc147356116)

[Crackstation 4](#_Toc147356117)

[Flag 1 5](#_Toc147356118)

[Python Exploitation 5](#_Toc147356119)

# Host Discovery

A black and white screen with white text

Description automatically generated

**Kali**: 192.168.56.101

**Victim**: 192.168.56.147.

# Nmap



A black background with white text

Description automatically generated



A computer screen with white text

Description automatically generated

# Viewing Website



This is the hint.

# Nikto



# Dirb

A black background with white text

Description automatically generated

# Exploitation

Since FTP allows anonymous login I can log into it. I notice that the /files/ directory contains CALL.html which also shows up in the FTP server. This means I can upload a file called shell.php to setup a reverse shell connection.

A screen shot of a computer

Description automatically generated

A computer screen with white text

Description automatically generatedNext, set up a reverse shell on the kali machine to listen to the same port.

Now I am in.

# Escalation

## Upgrade Shell

A black background with white text

Description automatically generated

A screenshot of a computer screen

Description automatically generatedIn the home directory I can see a txt file called important.txt.

## A screenshot of a computer Description automatically generatedFinding binaries



This was nothing of use.

## Finding the file



A screen shot of a computer

Description automatically generated

This is in the root directory.

This gives me the password for the shrek account.

hash: cf4c2232354952690368f1b3dfdfb24d

## Crackstation

Credentials – shrek:onion.



A close up of a date

Description automatically generated

Now I am inside the other user.

A screen shot of a computer

Description automatically generated

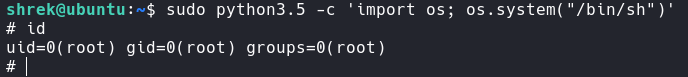
Given my current sudo permissions I can create a script that can spawn me a privileged shell.

# Flag 1

A computer screen shot of a person

Description automatically generated

# Python Exploitation

I thought I was being smart however I ended up writing a program that didn’t actually read the file. However the program read all of the files in the root directory and found the flag name. However It failed to read it. It did read the bash\_history file which showed a python one liner to escalation privileges. sudo python3.5 -c 'import os; os.system("/bin/sh")'.

A screen shot of a clock

Description automatically generated