Walkthrough - Template

Contents

[Host Discovery 2](#_Toc146577067)

[Nmap 2](#_Toc146577068)

[Nikto 2](#_Toc146577069)

[Dirb 3](#_Toc146577070)

[Viewing Website 3](#_Toc146577071)

[Stegseek 4](#_Toc146577072)

[Knock 4](#_Toc146577073)

[Exploitation 5](#_Toc146577074)

[Hydra 5](#_Toc146577075)

[Escalation 5](#_Toc146577076)

[Flag 1 5](#_Toc146577077)

[Finding Binaries 6](#_Toc146577078)

[LinPEAS 6](#_Toc146577079)

[ID 6](#_Toc146577080)

[LXC 7](#_Toc146577081)

[Root 7](#_Toc146577082)

[Flag 2 8](#_Toc146577083)

# Host Discovery

A black and white screen with numbers and a black background

Description automatically generated

**Kali**: 192.168.56.101

**Victim**: 192.168.56.148

# Nmap

A black background with white text

Description automatically generated



A screen shot of a computer

Description automatically generated

# Nikto









# Dirb



A screen shot of a computer

Description automatically generated

# Viewing Website

While viewing the source code of the default website <http://192.168.56.148> I found a comment in the source code:

<!-- "Please, jubiscleudo, don't forget to activate the port knocking when exiting your section, and tell the boss not to forget to approve the .jpg file - dev\_suport@hackable3.com" -->

**Username**: jubiscleudo? (this might be a possible username).

Email: [dev\_suport@hackable3.com](mailto:dev_suport@hackable3.com) (this might be a possible email)

There is a mentioned jpg which sounds interesting.

This is what was found.

<?php

include('config.php');

$user = $\_POST['user'];

$password = $\_POST['pass'];

$query = " SELECT \* FROM users WHERE user = '{$ user }' and pass = '{$password}'";

$result = mysqli\_query($connection, $query);

$row = mysqli\_num\_rows($result);

#Validate Account

if($row == 1) {

$\_SESSION[user] = $user;

header('Location: 3.jpg');

exit();

} else {

$\_SESSION[not\_authenticated'] = true;

header('Location: login\_page/login.html');

exit();

}?>



This directory had wordlist.txt which I believe will be used to crack one of the passwords.

This directory contains 1.txt. Which is base64: MTAwMDA=

The hash translates to 10000.

Contains images.



This once again contained some information about databases.

A screenshot of a computer program

Description automatically generated

In the CSS directory I noticed 2.txt. It contains BrainFuck.

++++++++++[>+>+++>+++++++>++++++++++<<<<-]>>>------------------....



In the file mentioned above with the php script. There is a hidden image called 3.jpg.

I downloaded it.

# Stegseek

A computer screen shot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generatedI used the hackpass file which was downloaded prior (in the backups directory).

This results in port 65535.

# Knock

With all of the values gathered, I can put this into knock.

**Command**: knock <host> <port> <port>

Re-scanning port 22 shows that it is now open.

# Exploitation

Now that the ssh port is open I can begin to use hydra to brute force the password for “jubiscleudo”.

## Hydra

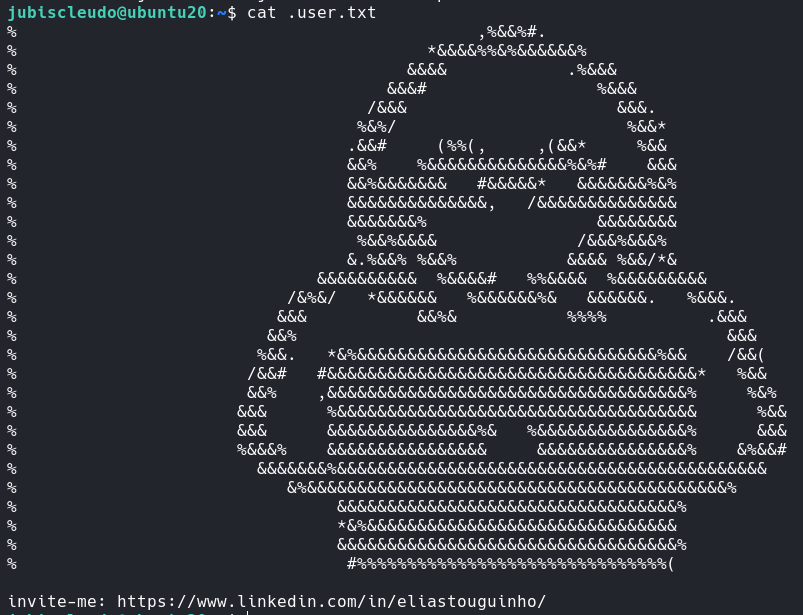
Password found.



# Escalation

In the home directory I found a secret file.

# Flag 1



I then setup a python server and downloaded les.sh into the system to determine what privilege escalation to begin.

A computer screen with white text

Description automatically generated

This would have worked, however there is no C compiler installed.

# Finding Binaries

A screen shot of a computer

Description automatically generated



In the home directory I noticed another user. This might be the user I need to exploit.

# LinPEAS

A computer screen with white text

Description automatically generated

**Credentials** – hackable\_3:TrOLLED\_3

I had to download this file using wget and python server.

# ID

A screenshot of a computer

Description automatically generatedI found out lxd is exploitable.

I found an exploit for it.

On the kali machine I must build it by calling sudo ./build-alphine.

# LXC





# Root



A black background with white text

Description automatically generated

# Flag 2

A person with a bow tie

Description automatically generated