Walkthrough – Evil Box 1

Contents

[Host Discovery 2](#_Toc146218191)

[Nmap 2](#_Toc146218192)

[Nikto 2](#_Toc146218193)

[Dirb 2](#_Toc146218194)

[FFuF 3](#_Toc146218195)

[Viewing Website 3](#_Toc146218196)

[Cracking SSH Key 4](#_Toc146218197)

[Exploitation 4](#_Toc146218198)

[Find Binaries 4](#_Toc146218199)

[Find Writable Files 4](#_Toc146218200)

[OpenSSL 4](#_Toc146218201)

[Flag 1 5](#_Toc146218202)

# Host Discovery

A black and white screen with numbers

Description automatically generated

# Nmap



A black sign with white text

Description automatically generated



# Nikto





# Dirb



A screen shot of a computer

Description automatically generated



I then searched for the extensions since that is what is required.

Found a file called evil.php. It is key to note that both index.html and evil.php have a response code of 200. This could be there are parameters. Which then we can turn to fuzzing.

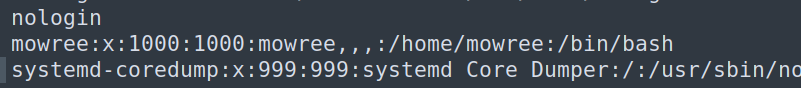
# FFuF

This command should reveal any hidden parameter that can execute the command /etc/passwd.

The result is command.

# Viewing Website

The secret directory doesn’t show anything, I don’t know why. There is nothing in the source code.

Robots.txt contains text that says “Hello H4x0r”. This text might be valuable later.

In the /etc/passwd file there contains an entry with ‘mowree’.

php://filter/convert.base64-encode/resource=evil.php

php://filter/convert.base64-encode/resource=index.html



A screenshot of a computer screen

Description automatically generated

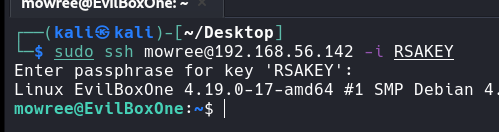
# Cracking SSH Key

A screenshot of a computer screen

Description automatically generated







NOTE: RSA key must be in the correct format, google the format if need be.

# A screen shot of a computer Description automatically generatedExploitation

## Find Binaries

I didn’t find any binaries besides su which peaked my interest however it wasn’t any use with the root password.

## Find Writable Files

**Command**: find / -perm -o+w 2>/dev/null

A screen shot of a computer

Description automatically generated



This means we can modify the file and add our own password to the root account.

## OpenSSL

A close up of words

Description automatically generatedGenerate a new password for root.

Add it.

Switch user.

# Flag 1

A group of white text

Description automatically generatedIn the root directory, the flag was waiting for me.