Walkthrough - Sahu

Contents

[Host Discovery 2](#_Toc149083935)

[Nmap 2](#_Toc149083936)

[Viewing Website 2](#_Toc149083937)

[Dirb 2](#_Toc149083938)

[StegSeek 3](#_Toc149083939)

[FTP 3](#_Toc149083940)

[Crunch 3](#_Toc149083941)

[FCrackZip 3](#_Toc149083942)

[SMBMap 4](#_Toc149083943)

[SMBClient 4](#_Toc149083944)

[SSH 4](#_Toc149083945)

[Passwd File 4](#_Toc149083946)

[Escalation 4](#_Toc149083947)

[OpenSSL 4](#_Toc149083948)

[Flag 4](#_Toc149083949)

# Host Discovery

# Nmap







# Viewing Website

A white background with black and white clouds

Description automatically generatedThe default webpage reveals a simple map along with text “Harayana”.

# Dirb



I noticed a pattern here, the first three letters of Haryana is spelt.



A blue and red text on a black background

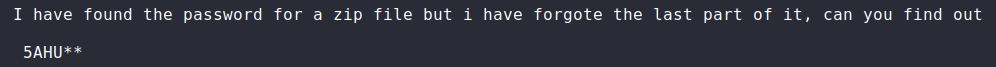
Description automatically generated

A valid webpage is returned. Viewing the source code reveals “Try to extract with hurrry”. Is this a tool? Or a password? I don’t know what it wants me to ‘extract’ but maybe content within an image.

# StegSeek

A computer screen shot of a computer code

Description automatically generated

**File Content**: “Haryana-1-1.jpg.out” 🡪 5AHU\*\*

A zip file password. Maybe there is a clue inside the ftp server.

# FTP

Since FTP anonymous is allowed and there is a file inside.

# Crunch

This tool can generate passwords based on given text or key words.

The following must be done:

crunch 6 6 -t 5AHU@, > passwords.txt

crunch 6 6 -t 5AHU@% >> passwords.txt

crunch 6 6 -t 5AHU@^ >> passwords.txt

crunch 6 6 -t 5AHU^@ >> passwords.txt

crunch 6 6 -t 5AHU,% >> passwords.txt

crunch 6 6 -t 5AHU^% >> passwords.txt

crunch 6 6 -t 5AHU%^ >> passwords.txt

# A screenshot of a computer Description automatically generatedFCrackZip

A screenshot of a computer program

Description automatically generatedPassword: 5AHU#5

Credentials – sahu:sahu14216

I tried to login using ssh but it didn’t work. Then I tried smb and it worked!

# SMBMap

A black screen with white text

Description automatically generated

Now I can use SMBClient.

# SMBClient



A black background with white text

Description automatically generatedThere is an ssh file that I can now access.

# SSH



Type in the provided password from the text file, then you are in.

# Passwd File

While I was looking for suid binaries, and capabilities I decided to look at the permissions for the shadow and the passwd file. The passwd file has write permissions, which means I can create an account.

# Escalation

## OpenSSL

A computer screen with white text

Description automatically generatedThe password is toor.

I then appended this to the passwd file.

A screen shot of a computer

Description automatically generated

# Flag

A black background with white text

Description automatically generated