**Walkthrough – Troll 1**

Contents

[Host Discovery 2](#_Toc147659501)

[Nmap 2](#_Toc147659502)

[Nikto 2](#_Toc147659503)

[The website 3](#_Toc147659504)

[Dirb 3](#_Toc147659505)

[FFuf 3](#_Toc147659506)

[FTP 4](#_Toc147659507)

[Wireshark 4](#_Toc147659508)

[Ghidra 5](#_Toc147659509)

[Hydra 6](#_Toc147659510)

[SSH 6](#_Toc147659511)

[Exploitation 7](#_Toc147659512)

[Upgrade Shell 7](#_Toc147659513)

[Finding Binaries 7](#_Toc147659514)

[Kernel 7](#_Toc147659515)

[Python Server 7](#_Toc147659516)

[Flag 8](#_Toc147659517)

# Host Discovery



A screen shot of a computer

Description automatically generated

**Kali Machine**: 192.168.56.101/24



A close up of a number

Description automatically generated

**Victim**: 192.168.56.133/24

# Nmap



A close up of a screen

Description automatically generatedNow I can re-run with those ports to discover service versions.

A screenshot of a computer

Description automatically generated

# Nikto

Since it hosts a website, this is a good vulnerability scanner.







There were two interesting files found.

# The website

The main website shows this image.

A screenshot of a computer

Description automatically generated

A cartoon face on a colorful background

Description automatically generatedRobots.txt reveals a secret directory.

Since the /secret/ is a directory and gives me an image there might be something hidden in this directory.

# Dirb



A screen shot of a computer code

Description automatically generated

This didn’t reveal anything of secret.

# FFuf



Also didn’t reveal anything secret.



# FTP

A screen shot of a computer

Description automatically generatedSince there is FTP available I will try anonymous login.

There was a file.

A screen shot of a computer

Description automatically generatedI will need wireshark for this.

# Wireshark

Opening the PCap file I was able to find these three packets.

A screenshot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generatedTurns out ‘sup3rsc3tdirlol’ is an actual directory.



# Ghidra

A screenshot of a computer

Description automatically generated

A white background with black and blue text

Description automatically generated

I realised that I could have used strings, however I found it regardless.

**Find Address**: ‘0x0856BF’

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

# Hydra

This might be a list of usernames and the password might be Good\_job\_:) or Pass.txt, or genphlux.



# SSH

A screenshot of a computer

Description automatically generatedSince the credentials are known: overflow:Pass.txt, I can just log into ssh.

# Exploitation

## Upgrade Shell



Quickly see if python3 is installed.

A black background with white text

Description automatically generated

## A screen shot of a computer Description automatically generatedFinding Binaries



I didn’t find anything useful and while looking I kept getting kicked out due to a timer.

## Kernel

Out of luck I decided to look at the kernel version and see if there was an exploit available. There was.

A black square with a white letter in the middle

Description automatically generated<https://www.exploit-db.com/exploits/37292>

## Python Server

I put it into a c file on my kali desktop and called it test.c. Next, I ran a quick HTTP python server on the machine based on my Desktop. This is so I can wget it in the /tmp folder of my kali machine.

A screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screen shot of a computer program

Description automatically generatedI then downloaded it onto the victims machine.

Compiled it.



Now I have root access. I can then go to the root folder and find the flag.

# Flag

A screen shot of a computer

Description automatically generated