Walkthrough - SlickOS

Contents

[Contents 1](#_Toc146928495)

[Host Discovery 2](#_Toc146928496)

[2](#_Toc146928497)

[Nmap 2](#_Toc146928498)

[Firefox Proxy 3](#_Toc146928499)

[Nikto 3](#_Toc146928500)

[Viewing Website 3](#_Toc146928501)

[3](#_Toc146928502)

[Exploitation 4](#_Toc146928503)

[Escalation 4](#_Toc146928504)

[Upgrade Shell 4](#_Toc146928505)

[Finding Binaries 5](#_Toc146928506)

[Web Directory 5](#_Toc146928507)

[Sudo -l 6](#_Toc146928508)

[Flag 6](#_Toc146928509)

# Host Discovery

# 

**Kali**: 192.168.56.101

**Victim**: 192.168.56.144

# Nmap

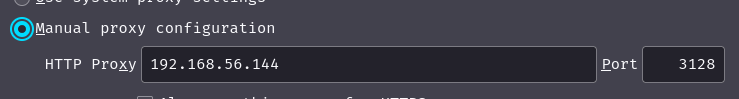
****



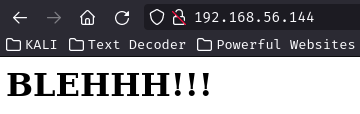
Looking here you can see that squid proxy is being used.



# Firefox Proxy



I added the following configuration to the network settings on my firefox browser.



This is what the website shows, if your proxy is working.

# Nikto

This scan contains the squid proxy port. The scan results in a massive output including robots.txt

Robots file contains the *wolfcms* directory.

# Viewing Website

# 

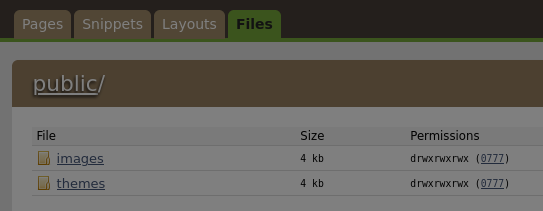
Looking at the source code for the *wolfcms* you will see a format where there is a question mark before the url. Example: /wolfcms/?/admin/login

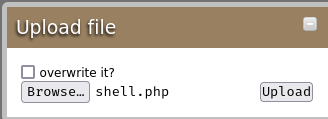
I tried the default credentials admin:admin and I was able to login.



# Exploitation

Now I have access to the dashboard I can go to the files tab and insert my own php file which will create a reverse shell.





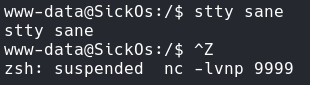
This should upload in the public directory of wolfcms.

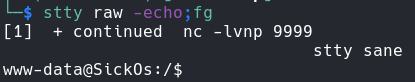


# Escalation

## Upgrade Shell

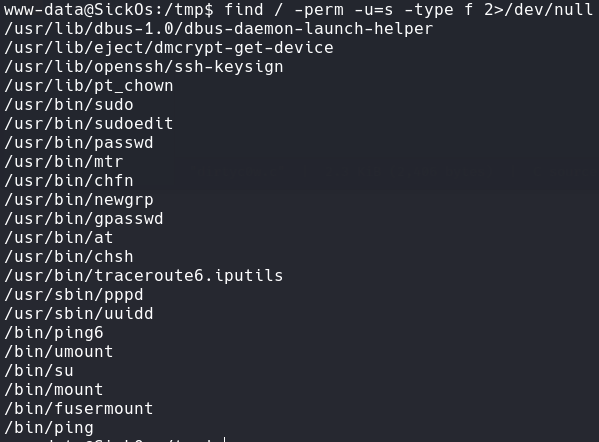






Now you have a proper shell with tab completion.

## Finding Binaries

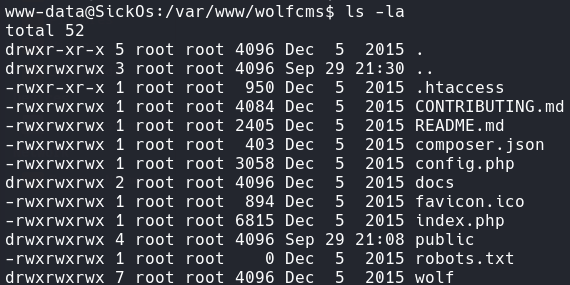


# Web Directory

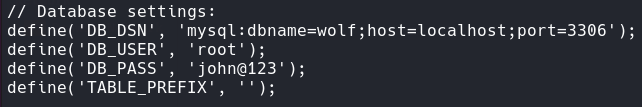


Connect.py is a database file from first appearance.

It contains the text that says I try to connect things very frequently.



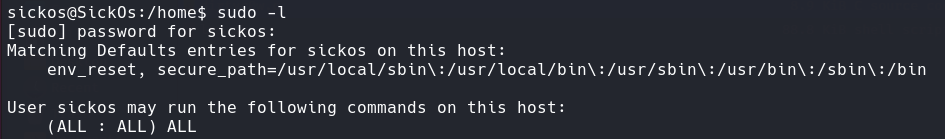
The config.php is interesting. I will cat the file to view the contents.





**Credentials** – sickos:john@123

## Sudo -l

I noticed I can run all commands as sudo, so that means I can simply write: sudo /bin/bash



# Flag

It is located in the root directory.



