Walkthrough - Eric

Contents

[Host Discovery 2](#_Toc145601413)

[Nmap 2](#_Toc145601414)

[Dirb 2](#_Toc145601415)

[Nikto 3](#_Toc145601416)

[Viewing Website 3](#_Toc145601417)

[GitTools 3](#_Toc145601418)

[Exploitation 4](#_Toc145601419)

[Upgrading Shell 4](#_Toc145601420)

[Flag 1 4](#_Toc145601421)

[Finding Binaries 4](#_Toc145601422)

[Linux Exploit Suggester 5](#_Toc145601423)

[Overwriting Script 5](#_Toc145601424)

[Flag 2 6](#_Toc145601425)

# Host Discovery

**Kali Machine**: 192.168.56.101/24.

A screenshot of a computer

Description automatically generated

**Victim**: 192.168.56.137/24.

# Nmap

A screenshot of a computer screen

Description automatically generated

There was a git repository found.

# Dirb

A screen shot of a computer

Description automatically generated

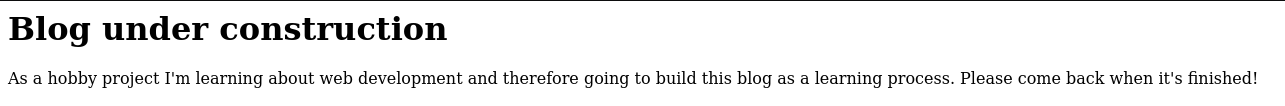
# Nikto





# Viewing Website

Default Page is: <http://192.168.56.137/>

The page source shows nothing of interest.

Admin.php is a login page. If you attempt to write in wrong credentials you are left with a message.

The /upload/ directory is forbidden, which most likely means there are files in there I can view.

# GitTools

Using gittools Ill download the entire /.git/ directory.





In this folder there is admin.php, which contains hardcoded password and username for admin.

admin: st@mpch0rdt.ightiRu$glo0mappL3

A screenshot of a computer

Description automatically generated

# A screenshot of a computer program Description automatically generatedExploitation

This dialog made me think I could add my own reverse shell. So I did and gave it a name. Then I thought how can I access this after I submitted? Then I looked at my notes and found /uploads/ and tried /uploads/shell.php and next thing I knew my netcat was connected.



## Upgrading Shell



Before I got this I tried python, and it didn’t work. Make sure to check the python version to avoid having to re-write entire command.

In the home directory of eric I see 3 files that are useful and a hint.

# Flag 1



For the script ‘backup.sh’ I tried appending a cat command to look for the flag, however it fails to execute.

# Finding Binaries



A screen shot of a computer

Description automatically generated

# Linux Exploit Suggester

I ran it and it found nothing.

A screenshot of a computer

Description automatically generated

# Overwriting Script





Now I can append it to the backup file.

I don’t know exactly who was responsible for what, however I ran the file using ‘sudo ./backups’ and then it failed because I don’t have the password for www-data. Then my netcat connected, to which it was now of id root. I tried previous times and failed, when I didn’t include sudo. I don’t know if this is because of an accident or because the backup.sh is scheduled to run.

# A computer screen shot of a black background Description automatically generatedFlag 2