Walkthrough – DC 9

Contents

[Host Discovery 2](#_Toc146403937)

[Nmap 2](#_Toc146403938)

[Nikto 2](#_Toc146403939)

[Viewing Website 2](#_Toc146403940)

[Wapiti 3](#_Toc146403941)

[SQLMap 3](#_Toc146403942)

[CrackStation 3](#_Toc146403943)

[Exploitation 3](#_Toc146403944)

[Hydra 4](#_Toc146403945)

[Escalation 5](#_Toc146403946)

[Binary Exploitation 5](#_Toc146403947)

[Sudo -l 5](#_Toc146403948)

[Test.py 5](#_Toc146403949)

[OpenSSL 5](#_Toc146403950)

[Root 6](#_Toc146403951)

# Host Discovery

A black background with white text

Description automatically generated

**Kali**: 192.168.56.101

**Victim**: 192.168.56.145

# Nmap







# Nikto



This is the only interesting things that were found.

# Viewing Website

A screenshot of a computer

Description automatically generated







# Wapiti





The tool found SQL injection within the site. I will then use SQLMap to find out more about this vulnerability.

# SQLMap



A screen shot of a computer

Description automatically generated

I found that you can either use the login page or the search page request and put it into sqlmap and find the databases.



A black background with white text

Description automatically generated



A black background with white lines

Description automatically generated

## CrackStation

admin:transorbital1

# Exploitation

After logging into the <http://192.168.56.145/manage.php> page I am now inside the website and can view records and search or manage.

When I add a new employee it adds it into the Staff database into the Staff Details table.

A black rectangle with white text

Description automatically generatedThis is an interesting thing, “file doesn’t exist” could mean that there should be something that loads when the page is loaded. Maybe there is a file parameter.

After some attempts I got it.



A black background with white text

Description automatically generated

The contents of the passwd file is exposed. I can see all of the users have accounts with valid shells.



This enables the ssh port to open up.



# Hydra

A close up of a login screen

Description automatically generatedThe usernames file contains the user accounts from the /etc/passwd.

These are the passwords I found.

I logged into all of them and saw nothing on the first two home directories. I did find something in janitors home directory.

A screen shot of a computer

Description automatically generated



# Escalation

## Binary Exploitation

A screen shot of a computer

Description automatically generated

## Sudo -l

## Test.py

A computer screen with white text

Description automatically generated

Reading this python file I can see that it takes in a file to read, then it will append the text to another file. This is possible to add another user to the /etc/passwd file with root privs.

## OpenSSL

Then after a hash is created, I can then add it to a file.

Credentials -> pwned:password

# Root

A black background with white text

Description automatically generated

Now I have root I can get the final flag.

A screenshot of a computer

Description automatically generated