**VulnHub – DrippingBlues Walkthrough**

Contents

[Host Discovery 2](#_Toc145326180)

[Nmap Scanning 2](#_Toc145326181)

[Nikto 3](#_Toc145326182)

[Robots.txt 3](#_Toc145326183)

[Dirb 3](#_Toc145326184)

[FTP 3](#_Toc145326185)

[FCrackZip 4](#_Toc145326186)

[File Inclusion 4](#_Toc145326187)

[Exploitation 5](#_Toc145326188)

[Flag 6](#_Toc145326189)

# Host Discovery



A screen shot of a computer

Description automatically generated

On the kali machine, using “ip a” I obtain the IP-Address: 192.18.5.101/24.

A black background with white text

Description automatically generated

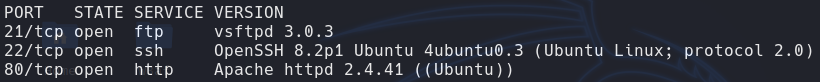
The victim machine is: 192.18.5.130/24.

# Nmap Scanning

A black background with white text

Description automatically generated

Now do another scan to determine the services and version.



Viewing the Site

A screenshot of a computer

Description automatically generatedThe site states that it has been hacked and there is a message left on it.

I am thinking of hidden directories and nikto.

# Nikto

The scan shows that there is a robots.txt.

A screen shot of a computer screen

Description automatically generated

## A screenshot of a computer Description automatically generatedRobots.txt

# Dirb

A computer code with white text

Description automatically generated

Dirb only found two valid (code 200) urls.

# FTP

A screenshot of a computer

Description automatically generatedAfter using some other directory enumeration tools I thought I would give FTP a try.

Turns out Anon FTP is enabled.

A black background with white text

Description automatically generated

Turns out there is a file that is zipped.

A computer screen shot of white text

Description automatically generated

It appears to need a password.

A screenshot of a computer

Description automatically generatedGoing back to the nikto scan I was able to view this file

There are 40 n words. I couldn’t get passed this so I went an attempted to brute force the password for the zip files discovered before.

# FCrackZip



Due to this tool not utilising the GPU, it will take some time. However, I was able to retrieve the password for one of the zip files.

Opening the file shows:

A screenshot of a computer

Description automatically generated

I will now run it for the ‘secret.zip’ file.

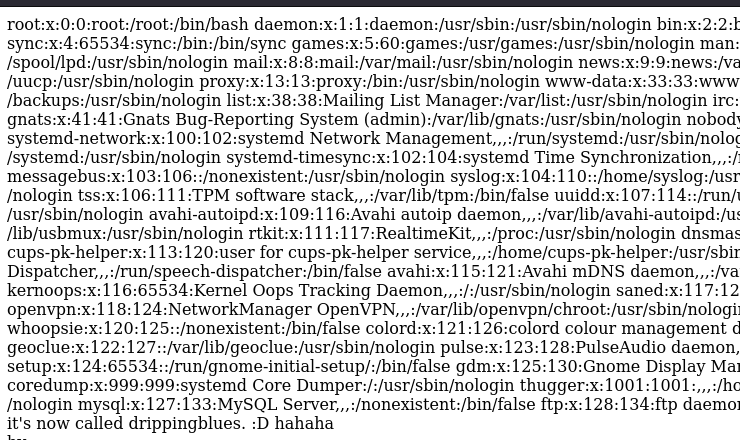
However I was unable to find any passwords.

# File Inclusion

I was looking around and thought about trying some file inclusion.



Since the previous hint said focus on ‘drip’ I thought it might be a directory, parameter or some form of sql hint. Then I tried to typical passwd file inclusion and it worked.



A screenshot of a computer

Description automatically generated

Since that /etc/passwd worked I thought about robots.txt and then tried the disallowed file.



The password would be for ssh. However What username it associates with requires me to inspect the passwd file again. I keep seeing thugger and traviscott. So I tried looking for both, and only thugger has an account. Which also worked on the physical vm.

# Exploitation



Once inside I found user.txt.



5C50FC503A2ABE93B4C5EE3425496521

I tried looking at the bash history and found that su root was an entry, so I used to above user.txt content as the password, but it didn’t work.



I tried to find some exploitable binaries.

I did find something that looked interesting and with a quick google search I found an exploit on github. The binary I found is Polkit.



I made sure that I did all of this is the tmp directory to ensure that I can create and run files.

After running the exploit I was able to switch user into Ahmed. Then switch into root.

# Flag

A screenshot of a computer

Description automatically generated



I found the flag.