Walkthrough Jangow

Contents

[Host Discovery 2](#_Toc145451256)

[Nmap 2](#_Toc145451257)

[Nikto 2](#_Toc145451258)

[Viewing the Website 2](#_Toc145451259)

[Dirb 2](#_Toc145451260)

[FFUF 3](#_Toc145451261)

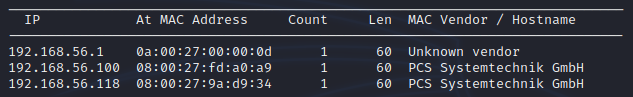
[Exploitation 3](#_Toc145451262)

[Privilege Escalation 4](#_Toc145451263)

[Finding Flag 5](#_Toc145451264)

# Host Discovery

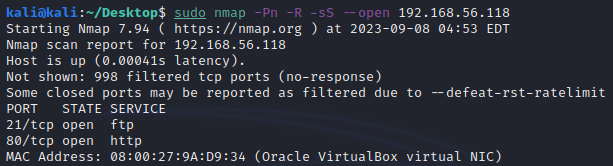




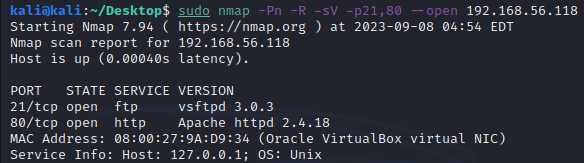
The victim machine is 192.168.56.118.

The Kali machine is 192.168.56.102.

# Nmap

The available ports are 80 and 21. These are file transfer and website.

Performing another one with the specified ports to detect the service version.



# Nikto

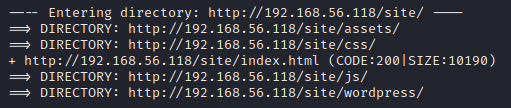
This didn’t reveal much.

# Viewing the Website

Viewing the website reveals a directory listing.

I viewed it for a bit and realised that I should probably enumerate it finding possible files/folders that can exist.

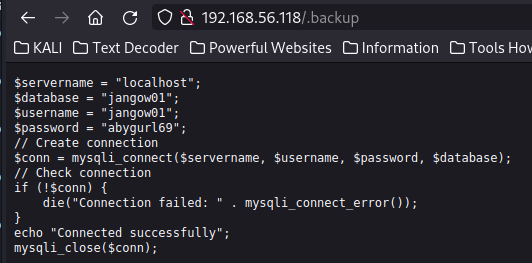
# Dirb



# FFUF

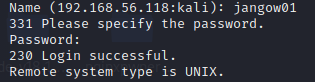


This will look for possible directories. Before I got this exact url and configuration I enumerated all of the possible directories my original dirb found. Then I found a common theme where they used a ‘.’ to hide files.



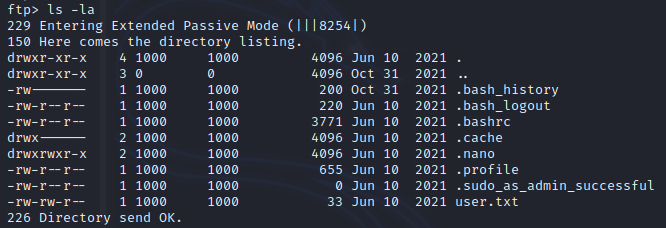
Since I don’t see a port open for mysql connection, I will look at the other protocol available one FTP.



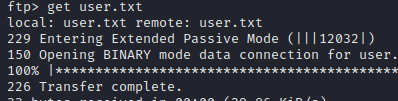


The credentials above logged me into the ftp server.

# Exploitation

Now that I am in the FTP server I can look into the home directory to see if there is anything I can use.

User.txt is the file that looks interesting, and I see a hint that we must sudo as admin to get the root flag.

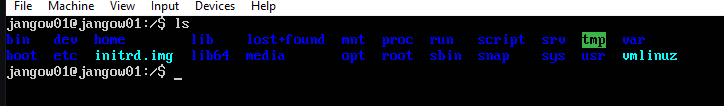
Get the flag.



This looks to be a password maybe.

I looked further and couldn’t find anything of use.

Then I tried logging into the actual virtual machine given the credentials above.



I am in.

# Privilege Escalation

To begin I will look for possible binaries to exploit.

Using the ‘find / -perm -u=s -type f 2>/dev/null”, but it saw no results.

I couldn’t find anything useful, and I spent some time just trying every binary and researching. Yet, I thought about the possibility that there might be a kernel level exploit. Using the command “uname -a” I was able to get the kernel version.

This exploit comes with a c file that can be uploaded to the server (using ftp) and compiled on the logged in victim VM.

A screen shot of a computer program

Description automatically generated

Compile it.

A screenshot of a computer

Description automatically generated

Now I tried to ‘id’ myself and it showed that the exploit has worked. I now have root access to the server.

# Finding Flag

A screenshot of a computer

Description automatically generated

Now for the root flag, navigate to the root directory and ‘ls’ the contents. The flag should be called ‘proof.txt’.