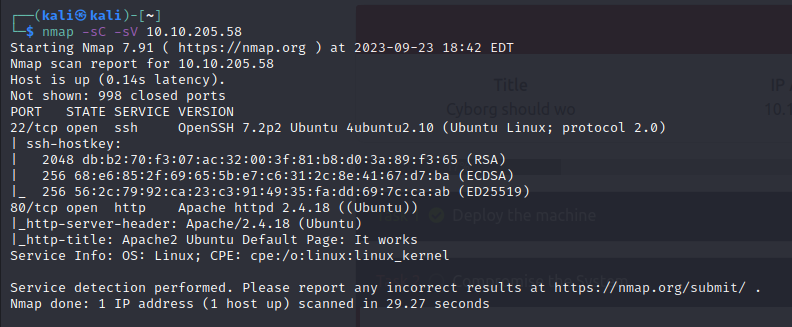
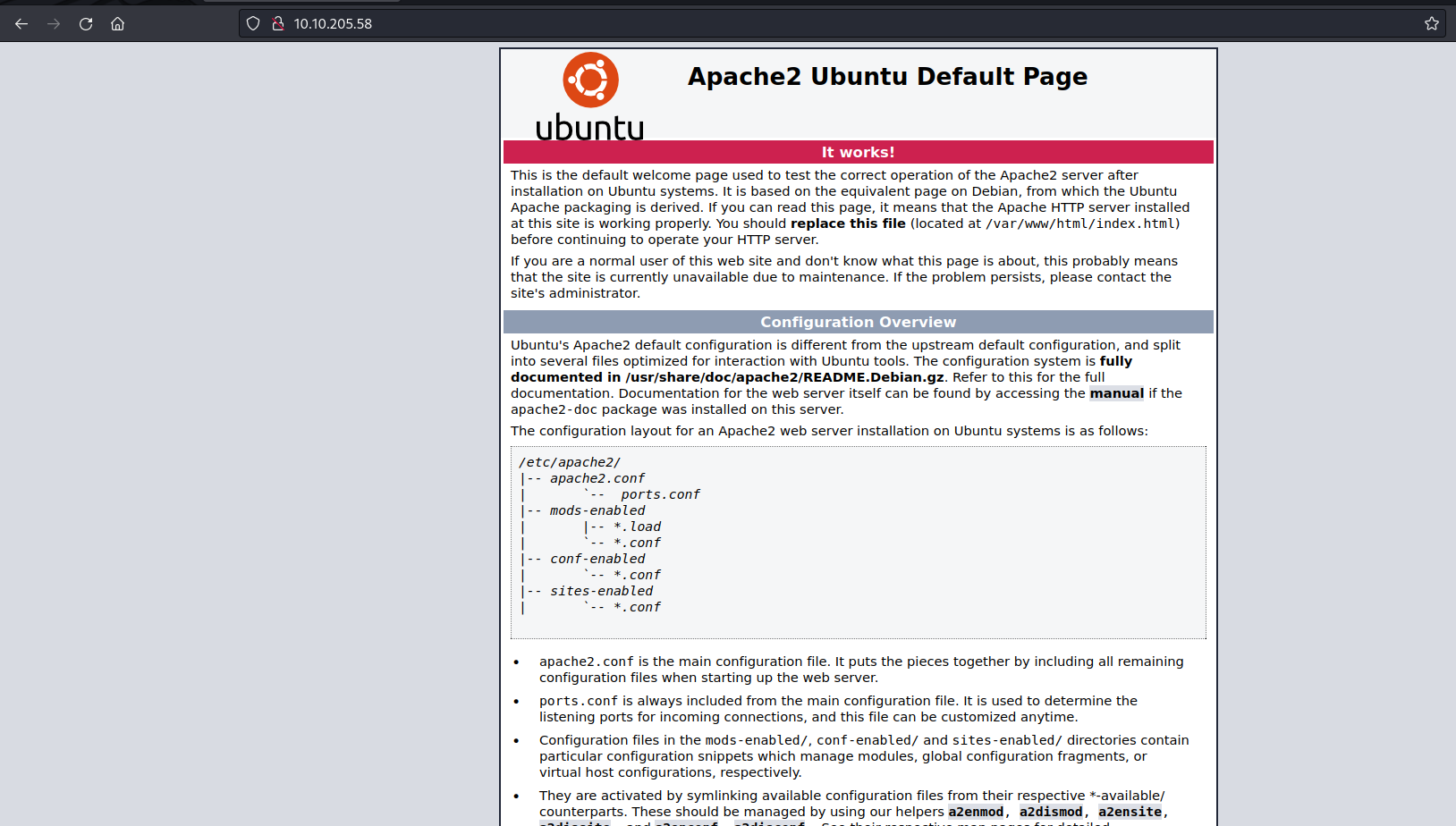
**Enumeration**

**Problem: Scan the machine, how many ports are open?**

1. Nmap -sC -sV (machine ip)

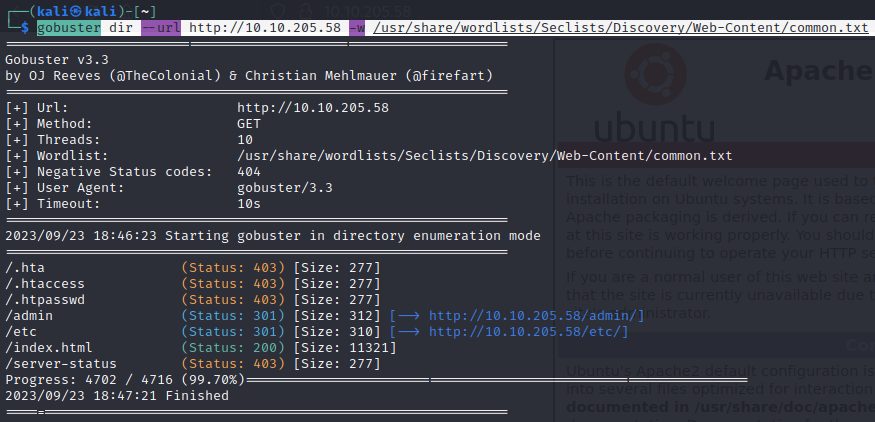


Looks like we’ve got a website and an ssh. Let’s check out the website.

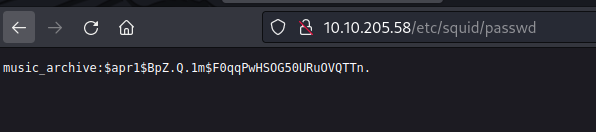


Seems it’s an Apache2 website. Let’s see there’s any subdirectories for us to look at.

1. gobuster dir --url http://10.10.205.58 -w /usr/share/wordlists/Seclists/Discovery/Web-Content/common.txt



Admin and etc look important here, let’s see them.



In the /etc/, we’ve found a squid folder. And in that a passwd folder. We’ve got a password of some sorts. Let’s keep note of it by making a “hash” file containing that password.

While in the /admin/ we find a download area in the archives tab. Which gives us a .tar. And in this is a config file. Showing:

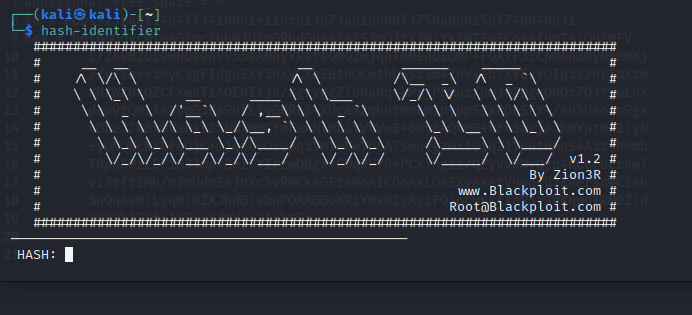


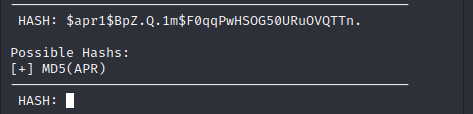
Let’s also keep note of this.

Now let’s crack that password for that music archive folder we found:

1. hash-identifier

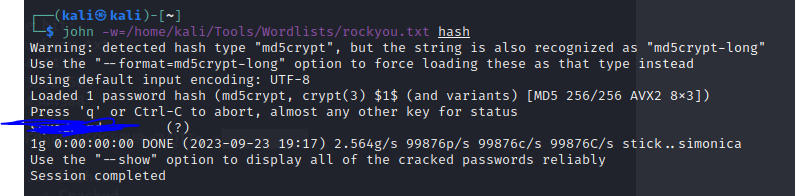
Now we just put in that has we got:



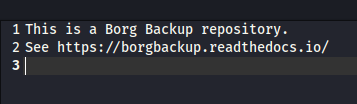


Looks like it’s an MD5 encryption. Let’s break it now.

1. john -w=/home/kali/Tools/Wordlists/rockyou.txt hash



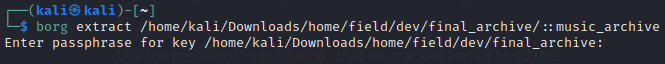
Alright we’ve got the password. Where can we use this though? The admin files we got before.



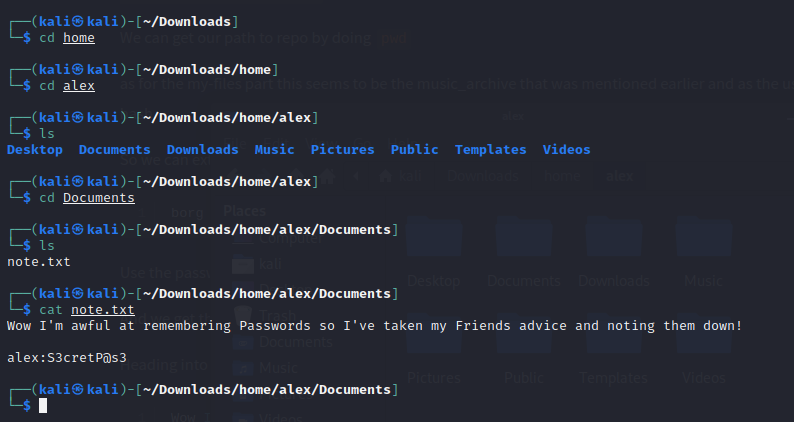
Here we see it’s got borg backup repository. I believe there’s something on github like this. Let’s install it now w/ “sudo apt-get install borgbackup”

Once we read that link, we see there’s an extract. That sounds useful. So let’s extract the archive with the credentials we got from /etc/

1. borg extract /home/kali/Downloads/home/field/dev/final\_archive/::music\_archive

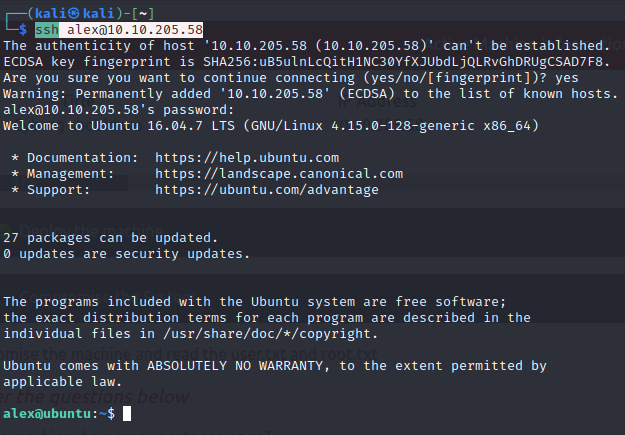


As you can see it asks for a passphrase. That passphrase we got from hashcracking the password before. So now we see there’s a new file in home! Let’s check it out.



Looks like we’ve got more credentials. Now remember how there was an SSH before in the nmap scan. Maybe it’s for that.

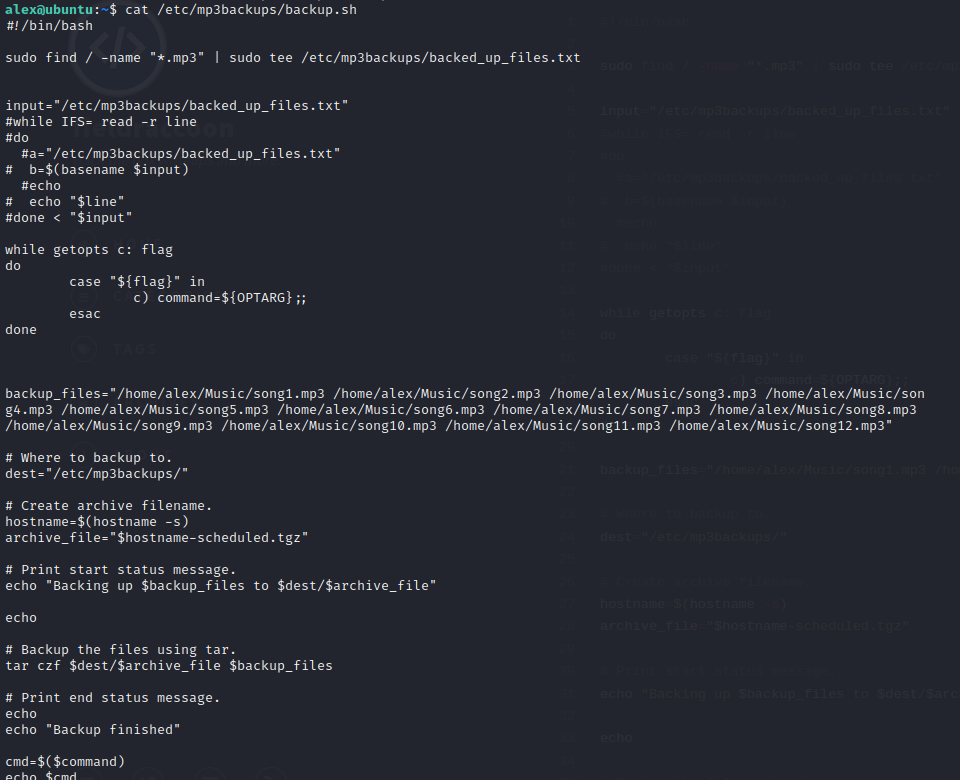
1. ssh [alex@10.10.205.58](mailto:alex@10.10.205.58)



And now we’re in! Now we just ls around and we should get our first flag!

**Privilege Escalation**

1. sudo -l



In this we see in the center with the “while” function that the command goes off of -c (the command line) and at the bottom we see it being executed.

Thus we shall use it!

1. sudo /etc/mp3backups/backup.sh -c whoami



As seen below, we executed the command we were permitted to run in sudo -l along with the -c at the end. And just so we could make sure it worked, we ran to “whoami” to tell if we actually ran it as root or not.

Now we actually become root.

1. Sudo /etc/mp3backups/backup.sh -c “chmod +s /bin/bash”

This let’s us make an executable bash

Now we open the shell:

1. bash -p



Now we find the flag and we’re all done!