Exercise 1

Esteban Calvo

2023-09-06

Contents

1 Attack Narrative

1.1 Key 1

To get key one, there were several steps that need to be parsed together to get the final file name. Firstly, we are told that we are searching for a file but don't know where, therefore we can start with using the unix command

```
find / -type f -name "KEY*"
```

which is going to the root directory and finding a file that matches the regex KEY* which in our case is KEY001. Once we do this, there are too many files that are restricted, so we can redirect the error messages to the dev/null. Once we have all the commands together, we get

```
find / -type f -name "KEY*" 2>/dev/null
```

and get the file /boot/grub/.hidden/KEY001-HcIGRLxTkUEkQVENTLN3za== and thus **key 1 = HcIGRLxTkUEkQVENTLN3za**.

1.2 Key 2

For this key, we are told to search the man files for a command the removes the "must have a tty" restriction. After some trial and error, the command

```
man ps | grep "must have a tty"
```

revealed ps -x is the command we want to use. To make it easier to find the key, the command

```
ps -x | grep "KEY002
```

is used and thus the result of KEY002 = u+9loQ38tAbuRZJbIHcKpQ.