Ex010 Report

Benjamin Ruddy

2022-09-09

Contents

Goal

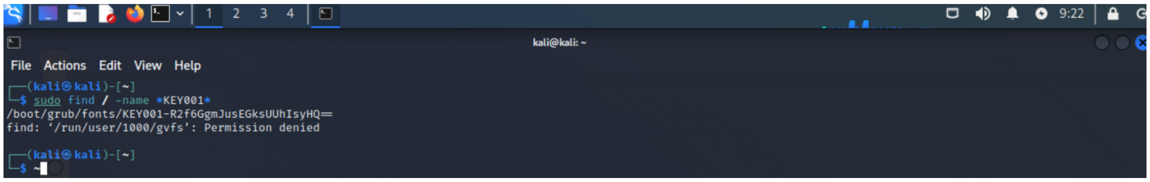
The goal in Ex010 was to find two distinct keys on the given Kali machine. The following attack narrative summarizes this procedure along with the commands that were used.

Attack Narrative

As per the instructions for the exercise, KEY001 formed part of a filename within the filesystem of the Kali NDG machine. Many commands could be used both individually or in combination to find the file, but I opted to go with the suggested `file` command to construct the following expression:

```
sudo find / -name *KEY001*
```

- The command was run with `sudo` to avoid any output about denied permissions.
- The / directory was specified to search from the root of the filesystem
- `*KEY001*` was specified to match against any output that had the string "KEY001" regardless of what characters came before or after it.



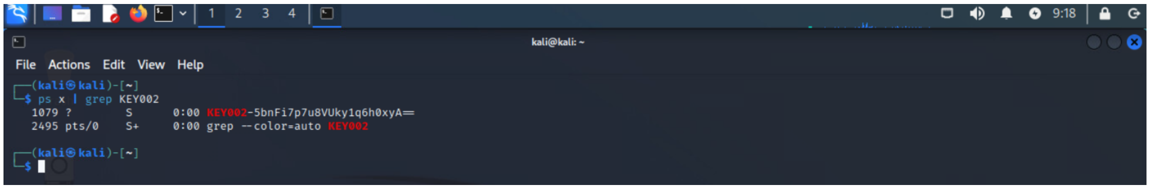
```
┌──(kali㉿kali)-[~]
└─$ sudo find / -name *KEY001*
/boot/grub/fonts/KEY001-R2f6GgmJusEGksUUhIsyHQ==
find: '/run/user/1000/gvfs': Permission denied

┌──(kali㉿kali)-[~]
└─$ ~
```

Figure 1: KEY001 being found with the above command

Moving on to KEY002, we are given the hint in the exercise briefing that there is a man page belonging to one of the commands in the slides for lecture 0x080 that has an argument that "lifts the *must have a tty* restriction." After some digging, we find that the `x` argument for the `ps` command fits this description. As it turns out, KEY0002 is a process, unlike KEY001 which was a file.

```
sudo ps x | grep KEY002
```

- The command is run with `sudo` for similar reasons to the first command
- The output of `ps  x` is piped into `grep` to specifically filter for output with 'KEY002' in it.



```
┌──(kali㉿kali)-[~]
└─$ ps x | grep KEY002
   1079 ?        S      0:00 KEY002-5bnFi7p7u8VUky1q6h0xyA==
   2495 pts/0    S+     0:00 grep --color=auto KEY002

┌──(kali㉿kali)-[~]
└─$ 
```

Figure 2: KEY002 being found with the above command