Ex010 Report

Benjamin Ruddy

2022-09-09

Contents

Goal

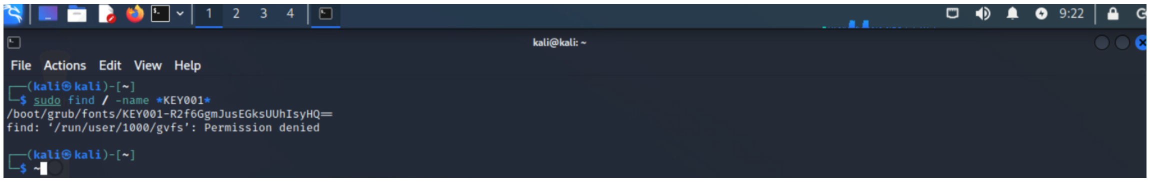
The goal in Ex010 was to find two distinct keys on the given Kali machine. The following attack narrative summarizes this procedure along with the commands that were used.

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.



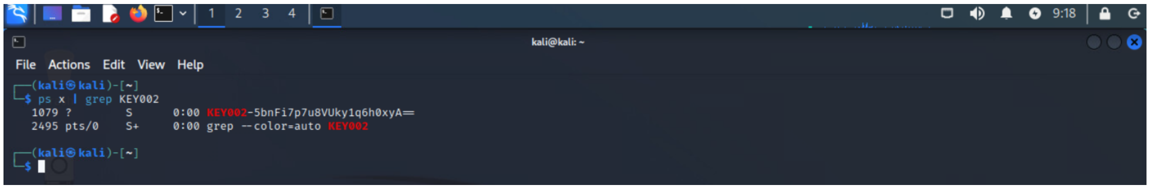
```
┌──(kali㉿kali)-[~]
└─$ sudo find / -name *KEY001*
/boot/grub/fonts/KEY001-R2f6GgmJusEGksUUhIsyHQ==
find: '/run/user/1000/gvfs': Permission denied

┌──(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

Ex020 Report

Benjamin Ruddy

2022-09-12

Contents

Goal

The goal in Ex020 was to devise two keys, KEY003 and KEY004, using information gained through OSINT (Open Source Intelligence).

Attack Narrative

KEY003

In order to arrive at the first key, it was necessary to first uncover the chiptune band that Joseph N. Wilson's son – *Person X.* – was a member of.

Given the name of the music venue that Person X. lived in, along with its city, the following Google search yielded a promising street address:

Google Search: `tv land tallahassee`

With the above search query, a Google Maps result comes up with the address **901 Buena Vista Dr, Tallahassee, FL 32304**, the next step was to uncover the past resident information to uncover Person X's identity. My first thought was to search through tax filings and property records, but as it turns out, this Google search revealed the answer before I even needed to search through those:

Google Search: `901 Buena Vista Dr "Wilson" Tallahassee`

Assuming that Joseph N. Wilson's son would have his same last name, we opt for the `"Wilson"` search term to filter out all pages that don't contain that piece of information. Prior to the above search, I attempted a similar one without the `"Wilson"` search term, and got mostly real-estate marketplace results, as opposed to sites that would offer more thorough information about the property's history.

From this, we are able to narrowed the name down to **"Thomas P. Wilson"** thanks to `https://clustrmaps.com/person/Wilson-7m3n87`, which additionally shows us four other past residents alongside Thomas. Having found Person X. as well as four potential people who may have been his bandmate, I iterated through the potential band members until I got a successful search from the following:

Google Search: `thomas wilson thomas clayton "chiptune" tallahassee`

The band **Melt Channel** seems to be a match, with both Thomas Wilson and Thomas Clayton being credited in the album "Erasers" (`https://meltchannel.bandcamp.com/album/erasers`), whose release date of 2015-12-08 matches the release date given to us. Noting that track number seven is called **Island**, we can devise the first key:

```
KEY003-F4D3onyBkoYdCzBcFrihpA==
```

KEY004

Using our knowledge of the band name that we got KEY003 with, finding KEY004 was a relatively straightforward process.

From Melt Channel's bandcamp page, we can look at their listed social media accounts to arrive at their Twitter page, `https://twitter.com/magic_circuit`, which has a post from 2018 announcing that "Melt Channel is now becoming **Magic Circuit**." Navigating to Magic Circuit's Twitter page, and from there to their Bandcamp page, we see an album release date that matches the second release date given to us (2022-02-25).

To discount the possibility of a coincidence, the following search was made:

Google Search: `"thomas wilson" magic circuit`

Given that multiple results list Thomas Wilson as a writer, along with the information from Melt Channel's social media posts, **Please Stay Connected**, the aforementioned album, was assumed to be the correct one from this new artist identity. Devising the key based on the featured artist on track six (**Gina**), and the instructions from task two of this exercise, yields:

```
KEY004-jfHIhklfispmr7p8HJ7Jew==
```

■