Sample: 6fd990

Sample

SHA256: `6fd9909f8ec81157735140283 2665d4a6b6e5399422b8cac79dd98532ac48913`

The sample is a an ELF file, its a modified copy of xhide which hides some given process.

- https://github.com/chenkaie/junkcode/blob/master/xhide.c

Task

What is this sample's intended purpose?

- The purpose is to hide a process

Static Analysis

Running floss and pestudio yielded the following results:

Notable Strings

```
You didn't think it would be that easy did you?
There is no usage statement here
path to fullness you seek
/dev/null
Error: /dev/null
Error: BigSpoon-1
Error: LittleSpoon-2
==> hammertime: %s Serial Number: %d
```

Libs

```
glibc
```

Dynamic Analysis

Fuzz Testing

I fuzz tested the sample with many inputs as args to understand what's trying to do.

strace

During the strace analysis I noticed that i tried to execute the given argument

`execve("/home/kali/Desktop/Samples4U/./6fd9909f8ec81157735140283266 5d4a6b6e5399422b8cac79dd98532ac48913", ["\1"], 0xff85c060 /* 54 vars */) = 0`

I also saw what does Serial Number prints

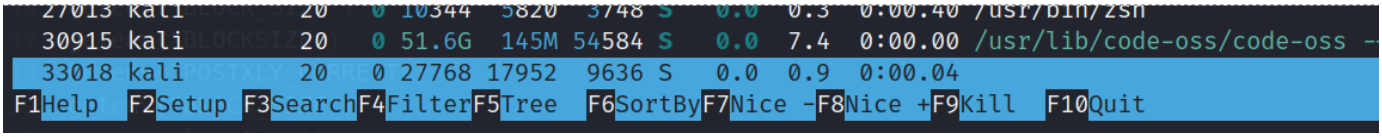
`getpid() = 38381`

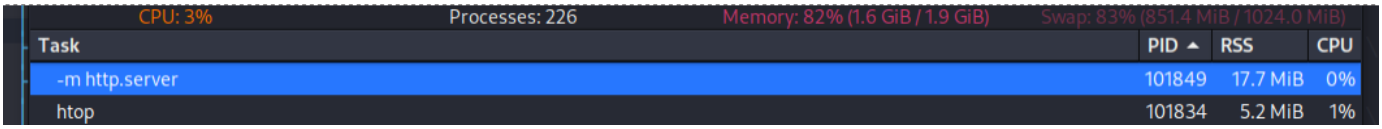
ltrace

Noticed that `ltrace` contains `waitpid(-1, 0, 0) = -1` which waits he child process to exit.

What the ???

I ran `htop` and the Kali's Task Manager to check if there is anything suspicious about the process and since that I ran the process with a python's web server `python -m http.server` I saw the PID in both of the outputs which derailed me from the right path a bit.





After a bit wandering, I realized that the exectuable name is missing.

Tools

- ltrace
- strings
- strace
- htop
- Gnome Task Manager
- Ghidra
- VirtualBox
    - KaliLinux