IT Security Engineering
Lab 8 - Unix Applications Security

November 7, 2014

Unix Application Security

SSH to appsec@lacalpe4.epfl.ch, password “appsec”.

You will find yourself with a few directories in your home. Each one of these is an exercise where you have to steal the secret value in a file you don’t have access to.

For each directory, there will be an SGID program that you can run. When a SGID program is run, the system will make it run with the rights of its own group, instead of the groups of the user running the program.

This is in general useful to allow users to perform specific tasks at escalated privilege levels, when the access control mechanism of the system is not fine-grained enough for a particular use case. Thus, it can become a serious security problem when a SGID/SUID program can be coerced into doing things that were not planned by the program author.

Your task is to exploit vulnerabilities in each of these programs, to force them to read and show you the contents of the secrets files that you are unable to access directly.

None of these require you to write a shellcode, or run any kind of bruteforce, or cpu-intensive code that will threaten the stability of the thing. If you think you require one of these, think again.

If you need a place to work, create yourself a directory under /tmp with a reasonably-hard-to-guess name.

We’ve tried to make the environment reasonably safe and concurrent, but if you find an unintended flaw, try not to ruin the setup for others :)

1