Internet of Things Security

FEI VŠB-TU Ostrava; Author: Ing. Vítězslav Grygar; Supervisor: Mgr. Ing. Michal Krumnikl, Ph.D.

Problem

The Internet of Things era is finally here. We are now surrounded by numerous devices monitoring or controlling the agriculture, industry, traffic and even health. This, however, imposes serious threat - malicious attacker able to control these devices can control our life to a great extent.

Solution

An IoT device is not that different from a classic computer - it must reliably provide desired function, store gathered data somewhere and communicate with other devices over a network. A great number of firmware rely on Linux, because it is an open-source (and therefore free), reliable, actively maintained, easily improved and proven solution. Unfortunately, reusing existing technology and software revives known flaws, often abusable by malicious parties.

Luckily, if certain system features are preserved, target can be analyzed in the same way as any Linux system. This is where Locasploit Framework comes in - it can detect software installed in target system by analyzing popular package manager databases. Names and versions of such packages are then compared against CVE - database of known vulnerabilities. Simple, yet efficient.

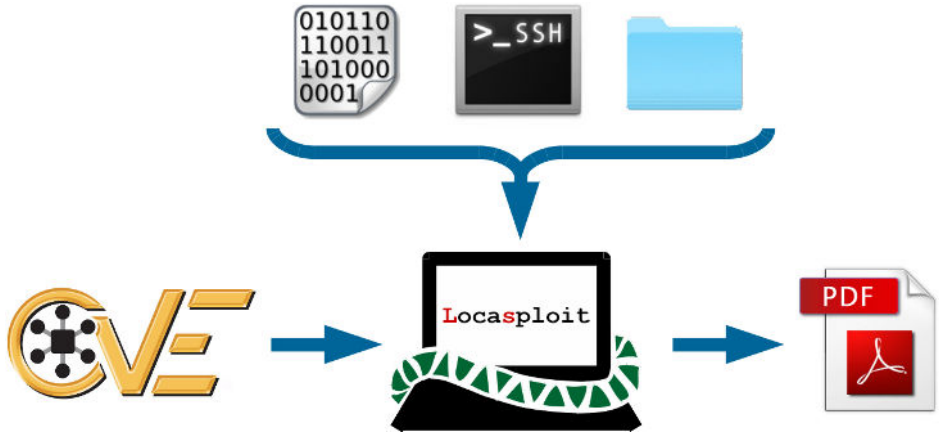
Resulting reports can be very comprehensive, mainly because of discrepancies between package information and the vulnerability database entries. There are several options to modify the Locasploit's behavior, nevertheless, false-positives are still present (and preferred over false-negatives). System administrators, firmware developers and penetration testers are the target audience.

Locasploit Framework

Introduced: 1/2016
Language: Python 3
License: GNU/GPLv2
Link: **https://github.com/lightfaith/locasploit**

Program Flow

As depicted below, CVE entries are fed into Locasploit. When analysis is in progress, Locasploit uses Binwalk to extract the target (if necessary), gathers basic system info and locates package manager database. Its content is then compared against pre-generated CVE database and the final PDF report is created.



Generally, Locasploit Framework can analyze samples that:
- are Linux-based,
- use one of the supported package managers.

The sample can be in form of:
- Binwalk-extractable binary,
- remote system accessible over SSH/SFTP,
- mounted/extracted/active root folder structure.

Results

Several publicly available firmware samples in binary form have been subjected to the vulnerability analysis. Locasploit has been able to successfully detect known vulnerabilities in 75 % of them. If used in real environment or with the aid of emulation software, additional 9.35 % of the samples would have been successfully analyzed.