Rootkit detection

Rootkit and trojan detection is performed using two files: `rootkit_files.txt` and `rootkit_trojans.txt`. In addition, other low-level tests are performed to detect kernel-level rootkits. You can use these capabilities by adding references to these files in `ossec.conf`:

```
<rootcheck>
    <rootkit_files>/var/ossec/etc/shared/rootkit_files.txt</rootkit_files>
    <rootkit_trojans>/var/ossec/etc/shared/rootkit_trojans.txt</rootkit_trojans>
</rootcheck>
```

These are the options available for the rootcheck component:

- **rootkit_files**: Contains the Unix-based application level rootkit signatures.
- **rootkit_trojans**: Contains the Unix-based application level trojan signatures.
- **check_files**: Enable or disable the rootkit checks. Default yes.
- **check_trojans**: Enable or disable the trojan checks. Default yes.
- **check_dev**: Check for suspicious files in the /dev filesystem. Default yes.
- **check_sys**: Scan the whole system for low level anomalies. Default yes.
- **check_pids**: Check processes for anomalies. Default yes.
- **check_ports**: Check all listening ports for anomalies. Default yes.
- **check_if**: Check interfaces for anomalies. Default yes.

Rootcheck helps you to meet PCI DSS requirement 11.4 related to intrusions, trojans, and malware in general:

> **11.4**: Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date. Intrusion detection and/or intrusion prevention techniques (such as IDS/IPS) compare the traffic coming into the network with known “signatures” and/or behaviors of thousands of compromise types (hacker tools, Trojans, and other malware), and send alerts and/or stop the attempt as it happens.

Use cases

Wazuh performs several tests to detect rootkits. One of them is to check for files hidden in /dev. The `/dev` directory should only contain device-specific files such as the primary IDE hard disk (`/dev/hda`), the kernel random number generators (`/dev/random` and `/dev/urandom`), etc. Any additional files, outside of the expected device-specific files, should be inspected because many rootkits use `/dev` as a storage partition to hide files. In the following example we have created the file `.hid` which is detected by OSSEC and generates the corresponding alert.

```
[root@manager /]# ls -a /dev | grep '^\.'
.
..
.hid
[root@manager /]# tail -n 25 /var/ossec/logs/alerts/alerts.log
Rule: 502 (level 3) -> 'Ossec server started.'
ossec: Ossec started.

** Alert 1454086362.26393: mail  - ossec,rootcheck
2016 Jan 29 16:52:42 manager->rootcheck
Rule: 510 (level 7) -> 'Host-based anomaly detection event (rootcheck).'
File '/dev/.hid' present on /dev. Possible hidden file.
```