Neo23x0 / auditd Public

Notifications Fork 258 Star 1.5k

Code Issues 15 Pull requests 25 Actions Projects Security Insights

master Go to file Code

Neo23x0 Merge pull request #134 from Pierr... c21d199 · 2 weeks ago 253 Commits

.github/workflows	Remove reference to patch-2 for pull r...	2 years ago
LICENSE	Initial commit	6 years ago
README.md	Update README.md	2 years ago
audit.rules	Merge branch 'master' into patch-63	2 weeks ago

README Apache-2.0 license

Maintenance Level Actively Maintained

```
    ___             ___ __      __
   /   | __  ______/ (_) /_____/ /
  / /| |/ / / / __  / / __/ __  /
 / ___ / /_/ / /_/ / / /_/ /_/ /
/_/  |_\__,_/\__,_/_/\__/\__,_/
```

Best Practice Auditd Configuration

Idea

The idea of this auditd configuration is to provide a basic configuration that

- works out-of-the-box on all major Linux distributions
- fits most use cases
- produces a reasonable amount of log data
- covers security relevant activity
- is easy to read (different sections, many comments)

Sources

The configuration is based on the following sources

Gov.uk auditd rules alphagov/puppet-auditd#1

CentOS 7 hardening https://highon.coffee/blog/security-harden-centos-7/#auditd---audit-daemon

Linux audit repo https://github.com/linux-audit/audit-userspace/tree/master/rules

Auditd high performance linux auditing https://linux-audit.com/tuning-auditd-high-performance-linux-auditing/

Further rules

Not all of these rules have been included.

About

Best Practice Auditd Configuration

- Readme
- Apache-2.0 license
- Activity
- 1.5k stars
- 82 watching
- 258 forks

Report repository

Releases

No releases published

Packages

No packages published

Contributors 27

+ 13 contributors

For PCI DSS compliance see: https://github.com/linux-audit/audit-userspace/blob/master/rules/30-pci-dss-v31.rules

For NISPOM compliance see: https://github.com/linux-audit/audit-userspace/blob/master/rules/30-nispom.rules

Video Explanations by IppSec

IppSec captured a video that explains how to detect the exploitation of the OMIGOD vulnerability using auditd. In that video, he walks you through the audit configuration maintained in this repo and explains how to use it. I highly recommend this video to get a better understanding of what is happening in the config.

https://www.youtube.com/watch?v=lc1i9h1GyMA

Contribution

Please contribute your changes as pull requests