Open-source software – Security concerns in a corporate environment

Dewayne Wasson

Davenport University

July 18, 2022

Professor Lonnie Decker

Abstract

The purpose of this study is to explore some of the potential impact of open-source software security concerns in a corporate environment. The study seeks to answer the research question, does open-source software affect the security posture of a corporate network? The goal is to analyze the potential impact to security using open-source software compared to any benefits available from its use.

Table of Contents

Chapter 1: Introduction

This study aims to identify whether using open-source software exposes a corporation to unnecessary security concerns and do the security concerns out-weigh the benefits of open-source. Open-source software can be implemented in any industry, from pharmaceutical to manufacturing environments. Licensing costs is one of the main benefits, however, the software must be obtained from a reputable source and maintained properly to ensure security concerns are addressed. In that respect, open source isn't different from commercially available software, patches and updates must be applied to address any existing or new security concerns. Open-source software addresses all relevant concerns of most organizations, providing benefits and an alternative to commercial closed source software.

Chapter 2: Literature Review

Internet research of studies and investigations already completed will be utilized to enhance this research paper and provide validation. Previous research can be an asset, using it to further my thesis and paper. Because of the large volume of previous research and documentation, using the literature to provide validity will be an asset to my research.

Open-source technology can be utilized and found in most any industry, from health care, manufacturing, to the technology arena. It can be used in many of the same ways or customized and implemented to address specific issues in the respective industry.

Software Licenses

The different types of licenses that are found with different types of software can be confusing. To be considered OSS, The Open Source Initiative defines that open-source software must follow several guidelines:

1. Free Redistribution – no restrictions on anyone trying to sell or give away the software.
2. The source code must be included as a true source as well as in a compiled form.
3. The license requires that modifications are allowed, and that the modifications can be distributed.
4. The original authors source code integrity must be maintained, distribution of the modified code can be restricted to ensure this integrity.
5. Everyone is allowed access to the software, no discrimination against anyone trying to obtain or use the software.
6. All fields of business are allowed to use the software, no discrimination based on type or nature of business.
7. The license applied to the original software is applicable, and no additional licenses are required.
8. Redistribution of the software maintains the license of the original software.
9. If other software is included with the licensed software, it must be free from restrictions.
10. The way the software is interfaced must not be restricted by any technology.

Table 1. Adapted from Open Source Initiative "The Open Source Definition"

Changing Corporate Trends

Historically open-source technology was believed to be lagging commercial options, but with crowd sourcing and large user communities, open-source matches commercial options in all avenues (Ruff, 2016). Ruff states that many large companies are seeing the benefits in both cost and security and are actively contributing to open-source projects. With large corporations

openly accepting and utilizing open-source projects, the use by other companies is spreading. Software vendors have found that releasing projects to the community, it also helps draw interest to the project and helps enlist programmers and contributors to the project (Ruff, 2016).

Most Popular Web Server

The Internet is a global implementation consisting of thousands of servers and resources offering information, data, and services to all who access it. Web servers make these resources available as users connect to them. Digital in the round states that open-source web servers are the most predominant currently on the Internet, powering over half of the web servers globally (2021). In 2021 Digital in the round released these statistics:

- Apache – 38.7% of the top one million sites
- Nginx – 32.1%
- Cloudflare Server – 14.1%
- Microsoft-IIS – 8.1%
- LiteSpeed – 6.5%
- Google Servers – 1.1%

Table 2. Adapted from Digital in the round "What Is the Most Popular Web Server Application?"

The Apache project had been the standard used web server for many years, but recently is being surpassed by another open-source project – Nginx. Open-source technology allows for an agile platform that can be quickly and conveniently adopted to needs and usage of both large and small implementations (Digital in the round, 2021).

Why Choose Open-Source Software

Boykin discusses the differences in perception of open vs. closed, or proprietary software, stating that there are five areas that may affect the choice of software that is purchased (2021) –

1. It must be cost effective to use and implement
2. Security of the software
3. Ability to integrate seamlessly
4. Overall quality of the software
5. Source code available

Table 3. Adapted from Tyler Boykin "5 Reasons to Choose Open-Source Solutions for Software Development"

Many times, smaller businesses cannot afford the cost of proprietary software, and open-source selections can fill the need they have. Along with the cost savings comes the cost of supporting the software, small businesses may not have the staff to support an open-source software selection. Without the staff, they may be more reliant on the support that comes with proprietary software. A small or limited budget may also influence a company to choose an open-source alternative over a proprietary choice (2021).

The large community and user base maintaining and monitoring the software ensures the quality and security of the software. The large number of eyes keeps the security and integrity of the software at a high level.

Cyber Security and Open-Source Tools

One area that was found to have open-source operating systems in prominent use is for security appliances and applications. Vendors like FireEye, Checkpoint, and Palo-Alto all make use of open-source technology as it makes an affordable platform that they can customize to their

needs and still know that they are providing a supportable, secure environment to their customers. Literature is not readily available on this subject without going directly to the vendors' sites and searching for their open-source disclosures.

Palo-Alto lists all OSS software that is used in its products and tools for reference in an available download, as does Checkpoint, FireEye, and many other securities tool vendors. OSS gives the vendors the ability to build their tools and modify the code to suit their intended needs and products. While many feel that having the source code being open to anyone to review it and break it down, using it as a base allows the vendors to build upon it, keeping cost down and making expandability inherent. Aaron Tan states that utilizing OSS allows security vendors to keep up with a rapidly changing cyber security environment and deliver more secure code as more eyes are involved in the development phase (2020). However, the software is only as secure as the users, community, and the vendors backing the software.

Chapter 3: Methods

Information for this research was gathered using several methods of collection. The primary means was through personal interviews of peers in the industry, getting their inputs and thoughts regarding the use of OSS in their lives. The researcher inquired of several individuals, and they are open to the interview, their inputs will be analyzed, compiled, and then incorporated into the final research paper. The survey will contain questions prompting them for their input on their use of open source and their experiences with it, while also allowing for an open discussion to allow the individuals an opportunity to openly express their feelings and thoughts. Proposed questions are:

1. Describe your experiences with open-source technologies in your work experience.

2. In your opinion, what was the main driving reason to migrate from closed source (HP-UX and/or Microsoft Windows) to Linux?
    a. Cost?
    b. Availability?
    c. Support?
3. Do you have any concerns about future support for Red Hat Linux or Amazon Linux?
4. Do you consider the current Linux to be more, less, or equally secure than closed alternatives?
5. Do you believe that Red Hat and Amazon Linux provide the same reliability and uptime as Microsoft Windows or HP-UX?

Using the same question source will ensure reliability of the answers and give a solid base for analysis. The interview will be concluded with an open discussion to allow the subjects to add any thoughts or concerns they have regarding the subject of open source.

Secondary research will also be used by utilizing and analyzing previous studies and research. Examining existing studies will allow me to use the results from them as a base and expand upon it with my research and evaluations. The data from the existing studies will also be analyzed for validity and thoroughness, to ensure that it pertains to and supports my research.

In addition to existing research and documentation, which proved to be an asset, as it helped show how the use and implementation of OSS has promoted and extended the cyber security field. The final means of research will be a physical implementation of an open-source platform in a lab environment, configuring a web server as one would be in a production environment. The guidelines for the experiment will be to assemble everything and build it

using all open-source software, then update and patch it just as a production environment would be. A Linux operating system will be deployed on a Virtual Box platform, then nGinx or the Apache web server would be deployed and configured. Once the system is up and serving up web pages, the Greenbone Vulnerability Manager, formerly known as OpenVAS, will be set up and configured on a Kali Linux system. The results from the vulnerability scans will be analyzed to show that a system composed of OSS can be a secure platform with which to deploy applications and resources.

Chapter 4: Results

Interviews

For this research two individuals were interviewed, both requested to remain anonymous and were willing to participate in this project. Both interviewees are currently involved in day-to-day support and engineering of both closed and open-source environments with a major manufacturer in the food industry. The first individual, who will be referred to as JB, described his experience as having over fifteen years of managing HP-UX and shared storage systems, having been involved with the deployment and management of a global Unix environment supporting a user base of over 20,000 users. Within the last year, they have actively participated in the migration of the environment from on-premises to cloud-based infrastructure in AWS employing Amazon Linux. JB stated that the reason for the migration from HP-UX to Linux was basically for financial licensing reasons. He also felt that the support available for Red Hat was comparable to what was available from HP. Red Hat offers a unique licensing model. While the software is indeed open-source, updates and support for it are only available when you purchase an agreement with them to provide the updates and support. Having a paid support program allows Red Hat to provide a dedicated staff to provide that support to their customers.

JB felt that Linux offered reliability, but not quite as good as when they ran HP-UX. He stated that with Linux, you had to ensure that the application and the OS had to be resilient to an unplanned server outage by utilizing high availability (JB, 2022). In this case, the closed source operating system proves to be superior to the open-source alternative. Linux would still be an option but would have to be designed to ensure system uptime and availability. Lastly, he stated that Linux would be an option for the end user provided that all the applications used are tested and proven to be compatible with the operating system.

The second interview was with a person that will be referred to as AG. AG is an active Linux engineer, designing and implementing Linux systems in a large corporate manufacturing environment. When discussing the reason for migrating to Linux, he stated that HP-UX requires dedicated hardware, and isn't flexible enough to be supported to run in a virtual environment. The current trend is to move away from physical data centers and utilize virtual servers in a cloud-based environment. Cloud migration allows the company to provide optimum uptime and remove the need for hardware support and upkeep. An important point that was brought up was in reference to patching the operating system for security vulnerabilities. AG stated that with HP-UX they only had to patch once yearly, whereas with Linux they are patching quarterly (AG, 2022). He did consider HP-UX to be slightly more stable than Linux, but with the advances being made with Linux, not by enough to not be considered an alternative. One other area that was brought up is application compatibility. One application that is currently in use is considered legacy as it isn't actively supported anymore but is essential to a shipping function that has yet to be migrated to a currently supported application. The application is old enough that it isn't compatible with Linux and requires HP-UX to function. Due to their data center exit strategy, they have resorted to running an HP-UX emulator on the virtual cloud-based Linux

platform to keep the application up and running. While satisfying the necessity to move the servers and applications to the cloud, this presents an additional layer of support and potential issues to support the legacy application.

While asking to remain anonymous, the author appreciated the input given during both interviews. They provided valuable knowledge and insight into their experiences with open and closed source operating systems in a corporate environment, their many years of experience gave credibility to their thoughts and concerns.

Experiment

Setting up the test systems to be used in my experiment consisted of deploying virtual machine images on VirtualBox installed on a Mac Book Pro. VirtualBox allows for the quick deployment of operating systems, giving the ability to generate snapshots of the guest OS that can be used to rollback to if changes go wrong and cause unexpected issues. Both operating systems were chosen to closely simulate what would be used in a corporate environment.

The first guest OS - Rocky Linux, was downloaded from the Rocky website as an ISO image to perform the installation of the OS. Rocky Linux is openly available for download at no cost and the source is obtained directly from Red Hat Enterprise Linux. Rocky is community maintained and a very stable platform for testing and development, and since it is derived directly from Red Hat source, it is very close to what would be run on a corporate production environment. The system was set up using default options and settings. Once setup was complete all updates and patches were applied to the system. The web server Nginx was installed, along with PHP web services to provide a running application on the server. Using a browser from a separate workstation, I was able to browse to the default web page for Nginx. A

PHP test web page was set up to show the status of the PHP service on the server, everything was accessible and showing as expected.

The second server was set up using software downloaded from the Fedora Project website. Fedora is also a distribution based on Red Hat Linux and strives to provide a stable platform that is 100% compatible with Red Hat. The set-up of Fedora was done like the Rocky Linux platform, all patches and updates were applied and kept up to date to ensure security and stability.

The system used to test the other systems for vulnerabilities was also an open-source option. Kali Linux can be obtained as an image from the Kali website with many open-source forensic tools installed and ready to use. The tools Kali provides can be used as forensic tools to evaluate systems in a defensive manner, or as offensive type hacking tools. In my experiment I am using Kali to check for vulnerabilities on systems using the Greenbone scanner. Greenbone is considered one of the top picks for open-source vulnerability management. The scanner can be used to test a network for over 100,000 vulnerabilities and can be updated to stay up with new vulnerabilities as they are found. The systems were set up to go through a full scan and be tested for all known vulnerabilities at the time of the test.

All the systems tested were found to have a low vulnerability score, so they were safe to be put into production on the network. Doing regular schedule testing and scans must be done to ensure that the systems stay up to date and remain secure. Regarding vulnerability scanning, proper care should be taken with the scan results. Allowing the scan results to get into the wrong hands is essentially handing all your known vulnerabilities over to a potential adversary. Care should be taken to ensure the results are kept confidential and secure. Utilizing encryption and ACL’s to ensure that only the proper teams and individuals have access to the results.

The first system assessment returned zero high level alerts, 3 medium, and 1 low. Depending on your security posture and how vulnerabilities are remediated, the system would be sufficient to be run in production and remediated soonest possible.

Host	High	Medium	Low	Log	False Positive
192.168.56.4	0	3	1	0	0
Total: 1	0	3	1	0	0

The three medium level alerts were for -

- The remote SSH server is configured to allow / support weak key exchange (KEX) algorithm(s).
- The remote SSH server is configured to allow / support weak encryption algorithm(s).
- The remote host is missing one or more known mitigation(s) on Linux Kernel side for the referenced 'SSB - Speculative Store Bypass' hardware vulnerabilities.

The report then gives references to research the issue and find remediation steps, this is the references for the first reported vulnerability -

References

url: https://weakdh.org/sysadmin.html

url: https://tools.ietf.org/id/draft-ietf-curdle-ssh-kex-sha2-09.html

url: https://tools.ietf.org/id/draft-ietf-curdle-ssh-kex-sha2-09.html#rfc.section.5

url: https://datatracker.ietf.org/doc/html/rfc6194

Having the vulnerabilities revealed and given the remediation steps allows the technician the ability to identify and remediate the issues correctly and accurately. The recommended updates were applied, and the system rescanned to show that all vulnerabilities were resolved.

The second system was scanned to find the following results -

Host	High	Medium	Low	Log	False Positive
192.168.56.6	0	1	1	0	0
Total: 1	0	1	1	0	0

This system was running the Apache web server, no vulnerabilities were found with it. The one medium vulnerability found was with the system kernel -

- The remote host is missing one or more known mitigation(s) on Linux Kernel side for the referenced 'SSB - Speculative Store Bypass' hardware vulnerabilities.

Upgrading the kernel to the latest available kernel resolved the vulnerability and the system was rescanned and found to be ready to return to service. Regular patching and updates will help keep systems up to date and address any security vulnerabilities. In addition to the Greenbone scanner, the OSS scanner Nessus was used to also scan the systems. Results from both scanners were found to be comparable.

Chapter 5: Conclusion and Recommendations

Open-source software is in our daily lives in many more ways than we imagine. Everything from smart TVs to the new smart coffee maker or refrigerator that was just purchased. The inner workings of these devices are more than likely utilizing an open-source operating system of some kind to connect it to the Internet and make it available for our use. The World-Wide-Web is composed primarily of open-source web servers and support systems. Corporations across the world utilize open-source to run many of their systems and use open-source tools to monitor and maintain the security of their infrastructures. The Internet is becoming more of a part of our daily lives, with the ways increasing every day. Ready or not, we must accept and endorse open-source technology, without it we would not be able to access and use many of the things we have become so accustomed to. As with any operating system or

infrastructure appliance, patching for security holes and vulnerabilities must be maintained and enforced. Allowing outdated hardware and software opens any environment up to potential issues as new vulnerabilities are exposed every day. Patching does not apply just to open-source solutions, but must be maintained in any environment, utilizing open or closed operating systems.

Overall, whether you choose to go with a closed or open-source operating system is entirely up to the corporation. Corporate guidelines and policies should be verified and confirmed before deciding on which platform to choose. Support can be a deciding factor when the corporation may not have a large internal IT support staff, therefore reliance on vendor support may be necessary and imperative to keep systems up and functioning at the accepted levels. Cost would be another factor to be considered, since implementing numerous servers and support systems on a closed source platform can potentially require a large budget and commitment.

To make a recommendation requires these factors to be considered and to adjust to what meets your business needs, which may be a mixture of open and closed source systems. One option is running closed source such as Microsoft Windows for the top tier applications, and Linux for all supporting systems. Alternatively, running open source for everything is also viable, provided the support is available to ensure maximum uptime. Whichever way is chosen, updates and patches are imperative and must be applied to all systems, regardless of operating systems. Patching can keep systems protected for known bugs and help when zero-day bugs are discovered.

References

Admin. (July 18, 2021). What Is the Most Popular Web Server Application in 2021? Retrieve March 27, 2022, from https://digitalintheround.com/what-is-the-most-popular-web-server/.

AG. Anonymous interview with the author. May 2022.

Babcock, C. (2000, May 1). Linux: Testing, Security Concerns Raised. *Inter@ctive Week*, *7*(17), 16. https://link.gale.com/apps/doc/A62023315/ITOF?u=lom_davenportc&sid=summon&xid=48d5310d.

Boykin, T. (June 6, 2021). 5 Reasons to Choose Open-Source Solutions for Software Development. Retrieve April 9, 2022, from https://techchannel.com/Enterprise/06/2021/5-reasons-open-source.

Dunlop, W. C. N., Mason, N., Kenworthy, J., & Akehurst, R. L. (2017). Benefits, challenges and potential strategies of open source health economic models. *PharmacoEconomics, 35*(1), 125-128. http://dx.doi.org.proxy.davenport.edu/10.1007/s40273-016-0479-8

Ebert, C. (2009). Guest editor's introduction: How open source tools can benefit industry. *IEEE Software, 26*(2), 50-51. http://dx.doi.org/10.1109/MS.2009.38

JB. Anonymous interview with the author. May 2022.

M. Ballhausen, "Free and Open Source Software Licenses Explained" in *Computer*, vol. 52, no. 06, pp. 82-86, 2019. doi: 10.1109/MC.2019.2907766 keywords: {open source software;licenses;computer security} url: https://doi.ieeecomputersociety.org/10.1109/MC.2019.2907766

Open Source Initiative. (no date). The Open Source Definition. Retrieved April 9, 2022, from https://opensource.org/osd.

Ruff, Nithya. (August 12, 2016). Trends in corporate open-source engagement. Retrieved March 10, 2022, from https://opensource.com/business/16/8/corporate-trends-open-source.

Tan, Aaron. (September 11, 2020). Cyber security is next frontier for open source. Retrieved April 9, 2022, from https://www.computerweekly.com/news/252488909/Cyber-security-is-next-frontier-for-open-source.

Thankachan, B., & Moore, D. R. (2017). Challenges of Implementing Free and Open Source Software (FOSS): Evidence from the Indian Educational Setting. *The International Review of Research in Open and Distributed Learning*, *18*(6). https://doi.org/10.19173/irrodl.v18i6.2781

Appendix A - Acronyms

ACL - Access Control List

AWS - Amazon Web Services

DVR – Digital Video Recorder

HP-UX – Hewlett Packard Unix

IoT – Internet of things

ISO – Optical disk image standard created by the International Organization for Standardization

Nginx – a web server that can also be used as a reverse proxy, load balancer, mail proxy and HTTP cache

OS – Operating System

OSS – Open-source software

Appendix B - URLs

Kali Linux - https://kali.download/virtual-images/kali-2022.2/kali-linux-2022.2-virtualbox-amd64.ova

Rocky Linux - https://download.rockylinux.org/pub/rocky/8/isos/x86_64/Rocky-8.6-x86_64-dvd1.iso

Fedora Linux - https://download.fedoraproject.org/pub/fedora/linux/releases/36/Server/x86_64/iso/Fedora-Server-dvd-x86_64-36-1.5.iso

GreenBone - https://www.greenbone.net/en/vulnerability-management/

Nessus - https://tenable.com/products/nessus/nessus-essentials

VirtualBox - https://download.virtualbox.org/virtualbox/6.1.34/VirtualBox-6.1.34-150636-OSX.dmg