# Five Linux Distributions With Tools for Audit

**Do you have something to say about this article?**

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

***http://bit.ly/2rV2E1a***

My father used to say, "Every job is easy with the right tool." Sage advice, but it presupposes that the right tool is available when needed. Sometimes it is not. The "right" tool might be unavailable, challenging (or expensive) to acquire, or out of reach. It is in situations like these where creativity and ingenuity can fill the gaps.

For example, on a recent vacation overseas, I broke my glasses. I was able to repair them using a travel toenail clipper. To say that is not the right tool is an understatement, but being creative in this way allowed me to see (with only a minimum of frustration) until I could get home to my backup pair. The point? Sometimes leveraging what is available can get us around obstacles that would otherwise be crippling to accomplishing our goals.

It is in this vein that it behooves auditors and assessors to know about repositories and collections of special-purpose, freely available tools that they can directly employ to help them in the course of conducting an audit. Believe it or not, there are dozens of such collections in readily accessible, easy-to-use formats that an assessor can just pick up and use to accomplish tasks they might have on their plate. This article identifies Linux distributions that, while their primary purpose is not necessarily audit-related in nature, do provide collections of hundreds or, in some cases, thousands of tools, many of which audit professionals might find valuable. In each case, both the distribution itself as well as an example of how an auditor might employ the tools distributed with it are highlighted in this article.

"IT BEHOOVES AUDITORS AND ASSESSORS TO KNOW ABOUT REPOSITORIES AND COLLECTIONS OF SPECIAL-PURPOSE, FREELY AVAILABLE TOOLS THAT THEY CAN DIRECTLY EMPLOY TO HELP THEM IN THE COURSE OF CONDUCTING AN AUDIT."

Of course, it bears saying that there are many more out there than those listed here—these are only a starting point. Likewise, there is only so much space available to highlight from among the many, many tools within each distribution (and note that the same tools may be present on more than one environment). That said, the hope is that providing a starting point can help both inform auditors of a potential resource and enable creative options for getting around challenges that might present themselves.

**Ed Moyle**
Is director of thought leadership and research at ISACA®. Prior to joining ISACA, Moyle was senior security strategist with Savvis and a founding partner of the analyst firm Security Curve. In his nearly 20 years in information security, he has held numerous positions including senior manager with CTG's global security practice, vice president and information security officer for Merrill Lynch Investment Managers, and senior security analyst with Trintech. Moyle is coauthor of *Cryptographic Libraries for Developers* and a frequent contributor to the information security industry as an author, public speaker and analyst.

## 1 BlackArch Linux

BlackArch Linux *(https://blackarch.org/)* is a penetration testing distribution built on the Arch Linux platform. Distribution as a "live" ISO and as a virtual image allows the user to rapidly launch the platform to make use immediately (or nearly so) of its more than 1,900 tools. While the specific tools are focused on penetration testing (as this is the distribution's primary purpose), there is no shortage of tools that might be of interest to an auditor or assessor. Tools such as ssldump or sslmap, for example, can help an assessor validate appropriate configurations for web servers, for example, by allowing them to observe that appropriate ciphersuites are in use and older protocol versions (susceptible to DROWN, POODLE and the like) are not employed. Likewise, tools such as nikto and crawlic can help ensure that a web server configuration is appropriate and in line with requirements (e.g., not containing credentials, temporary files and other undesirable configuration artifacts).

## 2 Kali Linux

The successor to BackTrack, Kali *(https://www.kali.org/)* is probably the best-known penetration testing distribution in that community. One of the advantages of using Kali specifically is that there is a large body of community-generated "how to" content including instructional videos on how to install the environment and how to employ its tool set. As with BlackArch, there are a number of tools that might be of use to an assessor; for example, a tool such as OpenVAS (an open-source vulnerability scanner) can be used to validate the configuration baseline for hosts on the network or to ensure that document patch management and release processes are being followed. A tool such as nmap can be used to validate that hosts are running only the appropriate services in accordance with defined configuration processes.

## 3 REMnux

REMnux *(https://remnux.org/)* is an environment designed for security professionals engaged in malware analysis. While most auditors and assessors will not have much call to actively analyze malware, that does not mean that the same tools cannot be of use for an audit task. Tools built into this platform include the network protocol analyzer Wireshark and the network regular expression parser ngrep. These can be used for a range of purposes including ensuring that data exchange is appropriately secured (e.g., that cleartext usernames/passwords are not exchanged).

## 4 DEFT or CAINE

Distributions that support forensic examination of systems can also assist an auditor in the work they do. For example, distributions such as the Digital Evidence and Forensics Toolkit (DEFT) *(www.deftlinux.net)* or the Computer Aided Investigative Environment (CAINE) *(https://www.caine-live.net/)* are, as one might expect, rife with tools designed to manipulate, view, investigate and otherwise analyze files and file systems. These tools can support efforts of interest to auditors such as evaluation of the appropriateness of file system permissions, validating the existence and operation of data protection tools (e.g., encryption), or any number of other file manipulation tasks.

## 5 SELKS

This last one, the SELKS platform *(https://www.stamus-networks.com/open-source/)*, is a bit more special-purpose than some of the others. SELKS is a "live" ISO (i.e., a bootable and preconfigured environment) designed specifically to run the Suricata intrusion detection system (IDS) as well as its associated ecosystem and tools. This means that, within a very short period of time, an assessor can stand up a preconfigured IDS/intrusion prevention system (IPS) environment. Why is this helpful in the case of an audit? There are a number of reasons, but the most obvious one is to validate the operation of detective controls, for example, if an auditor wishes to ensure that the IDS, advanced malware detection tools or other controls are operating appropriately. Having an "out of band" way to evaluate events can help as part of that process, particularly when used in combination with earlier distributions (i.e., to generate attack patterns that can be observed by IDS tools.)