Mike Jurendic

COP 4640 - Operating Systems Environments

Professor Jim Littleton

11/16/19

On the Review and Setup of Security Audit Using **Kali Linux**

**Introduction**

The article is a review on the operating system known as Kali Linux. The article also reviews typical concepts in cyber security including penetration testing, security analysis and security audits. The main purposed of this article is to demonstrate how powerful and useful of a tool Kali Linux can be in cyber security by talking about some of its’ wide array of tools and capabilities. Kali Linux can do more than simply Pen-Test. It can perform audits and help discover unknown vulnerabilities (zero-day) [2].

**History and Installation of Kali Linux**

Kali Linux is operating system that is a derivative of the Linux Distribution known as Debian. It was made by Offensive Security and Its’ license level is freeware and has over 600 penetration testing tools. The OS is installed typically as virtual machine on virtual machine management software, such as Oracle’s VirtualBox. It can also be run off a USB as a bootable drive. It is worth mention however, that the article doesn’t cover the fact it *can* be made the actual operating system of a computer. Although this is not recommended at all by professionals as Kali can easily cause damage or get someone in legal trouble over a few small mistakes [1]!

**Penetration Testing**

One of the main features of Kali Linux is penetration testing. This is the practice of testing the security of devices and their information by performing attacks typically done by hackers, while also trying to be creative like them as well. Typical attacks include SQL injections which involves exploiting database systems by using SQL queries to trick the system into giving the attack sensitive data, and another example of a typical attack is infamous Man-In-The-Middle attack which an attacker spies on data traffic (e.g. packet sniffing) and manipulates the way traffic is received by the other two parties. According to the article, Kali Linux can also aid in discovering zero-day vulnerabilities within systems. This means that Kali is not limited to linear ways of testing and can be used dynamically to aid creative minds in testing their own systems and discover vulnerabilities before other clever hackers can [2].

**Security Analysts, Security Audits and training**

The authors of the article mention how cyber security analysts must keep reinventing themselves like hackers do to keep themselves ready. Methodologies and tools are constantly being developed as the malicious continue to tinker. Therefore, security auditing tools were inevitable and have surfaced. Security Audit tools allow analysts to scan entire systems’ log files for vulnerabilities and make it less tedious as possible. An example of this is Lynis, an open-source software used to audit systems for security and gives red-flags based on what is picks up in areas like the file system. Kali Linux can also be used to train aspiring analysts or further supplement current analysts’ knowledge. There are many ways this can be done, like setting up vulnerable servers to be prone to attack for specific exploits to show in reality how the attack works, test OS specific OS vulnerabilities (this is common with Windows according to the article, as most of today’s PCs use Windows), etc.

**Conclusion**

The article has demonstrated that the Kali Linux operating system is a serious tool that can be used to benefit cyber security professionals immensely. Operating Systems like this are continuing to benefit society and even opening many doors for those wishing to pursue a career in cybersecurity by making training more accessible. Offensive Security even has a certification for Kali Linux called the PWK (Penetration Testing with Kali Linux) which is prerequisite for a well respect certification known as the OSCP (Offensive Security Certified Professional) [3]. Operating Systems, especially nowadays, have many possibilities for even the common folk given our tools and level of accessibility. If they can be specialized to the point for pure cybersecurity, there’s no telling what else is in store for computing in the future.

References

Still need to reference the article

[1] – Congleton, Nick. 2018. What Is Kali Linux, and Do You Need It? (February 6th, 2018) Retrieved November 2nd, 2019 from <https://www.maketecheasier.com/what-is-kali-linux-and-do-you-need-it/>

[2] - Gunawan, Teddy Surya. 2018. On the Review and Setup of Security Audit Using Kali Linux. Indonesian Journal of Electrical Engineering and Computer Science. Article 11, pages 51 – 59. DOI: 10.11591/ijeecs.v11.i1.pp51-59

[3] – Offensive Security. 2019. Penetration Testing Training with Kali Linux. Retrieved November 2nd , 2019 from <https://www.offensive-security.com/information-security-training/penetration-testing-training-kali-linux/>