# System Security Tools: Kali Linux

# 

Student's Name

Institution Affiliation

Department/Course

Date

Most organizations regard cyber-security as a significant priority. The increasing overreliance on technology to steer crucial organizational operations has resulted in the proliferation of cybercrime. Successful cyber threats result in potentially devastating impacts on firms and individuals, including financial loss, tainted reputation, compromised customer data, and business information. However, existing and emerging software are designed to protect against various types of cyber-security, including information security, application security, disaster recovery, network security, and operational security. The areas mentioned above must be protected against numerous types of threats, for example, malware, ransomware, phishing, and social engineering. Both open-source and commercial cyber-security software tools collectively play a critical role in protecting sensitive and private data or information of organizations and individuals. However, this paper concentrates on Kali Linux; an excellent fast-developing penetration testing tool firms use to scan networks and numerous information technology systems for potential vulnerabilities.

Kali Linux is designed to have more than 300 system tools for effective cyber-security auditing (Najera-Gutierrez & Ansari, 2018). Most tools within the Kali Linux package are executable; therefore, users enjoy the privilege of monitoring and maintaining their network wellness and security systems using customized clicks. Organizations and individuals that use Kali Linux tech stacks, for example, Studio666.descartes, Poison, and Ventx, enjoy unmatched benefits, such as not necessarily requiring a particular set of skills and knowledge to function (Stylianopoulos, Almgren, & Landsiedel et al., 2020). All user types, from highly experienced to newbies, can effectively use Kali Linux tech stacks to reinforce organizational security within existing networking architectures. Kali Linux does not require organizations to employ advanced cyber-security analysts or specialists. The overall role of an analyst in an organization is therefore restrained by simply ensuring that the system is running. Lastly, the software tool is readily available for use and can be acquired through open-source mechanisms. However, although Kali Linux comes with the benefits mentioned above, the software tool is less useful for general office work because the development lacks various tools needed for daily office routines. This could be described metaphorically by stating that the screwdriver cannot drive nails, plane, or saw because its work is constrained to a screw.

The Kali Linux installation process is fairly straightforward. It may be executed using various options, such as a bootable USB drive, hard disk install, virtualization software, or dual booting with an existing operating system. Najera-Gutierrez and Ansari (2018) indicate that any options mentioned above are achievable once the computer system meets the standards system requirements, such as memory size and installation location. Irrespective of the installation option chosen, the Kali Linux installation process is predominantly similar to installing a new operating system on the computer. Therefore, the process is relatively simple to system analysts or anyone with experience in computer operating systems. Kali Linux is licensed and available for use like other operating systems; it is, however, a standard tool used by hackers to gain illegal entry into existing system networks.

Stylianopoulos et al. (2020) attest that Kali Linux is primarily designed to protect systems against advanced penetration and "security auditing" (p. 46). Cyber-security threat analysts have the opportunity to use hundreds of tools compacted within Kali Linux to undertake different information security tasks, including security research, penetration testing, security auditing, reverse engineering, and computer forensics. Unlike other cyber-security tools, Kali Linux has the following advantages to system analysts; freely available, available packaged tools, open-source software, multi-language support, and customizable support. The multi-language support and customizable benefit allow system analysts and developers to fit into different system architectures and organizational models efficiently. Besides preventing access, analysts must acknowledge that certain authorized users may also present potential threats (Stylianopoulos et al., 2020). Therefore, Kali Linux is generally designed to increase network security by limiting access and resources by monitoring individual responsibility.

References

Najera-Gutierrez, G., & Ansari, J. (2018). *Web Penetration Testing with Kali Linux - Third*

*Edition* (3rd edition). Packt Publishing.

Stylianopoulos, C., Almgren, M., & Landsiedel, O. et al. (2020). Multiple patterns matching

for network security applications: Acceleration through vectorization. *Journal of Parallel and Distributed Computing*, *137*, 34–52.