**SCSA2409 - IOT AND CLOUD SECURITY LAB**

**Experiment 1 - A study of simulation tool based on the parameters of data security**

**Aim: To study about the Kali Linux simulation tool based on data security**

**Description:**

1. **Kali Linux:**

[Kali Linux](https://www.kali.org/) is an [open-source](https://www.kali.org/docs/policy/kali-linux-open-source-policy/), [Debian-based Linux](https://www.kali.org/docs/policy/kali-linux-relationship-with-debian/) distribution aimed at advanced Penetration Testing and Security Auditing. It [does this by](https://www.kali.org/features/) providing common tools, configurations, and automations which allows the user to focus on the task that needs to be completed, not the surrounding activity.

Kali Linux contains industry specific modifications as well as [several hundred tools](https://www.kali.org/docs/policy/penetration-testing-tools-policy/) targeted towards various Information Security tasks, such as Penetration Testing, Security Research, Computer Forensics, Reverse Engineering, Vulnerability Management and Red Team Testing.

Kali Linux is a multi-platform solution, accessible and freely available to information security professionals and hobbyists.

1. **Features**

* **More than** [**600**](https://www.kali.org/docs/policy/penetration-testing-tools-policy/) **penetration testing tools included:** After reviewing every tool that was included in Back Track, we eliminated a great number of tools that either simply did not work or which duplicated other tools that provided the same or similar functionality. Details on what’s included are on the [Kali Tools](https://www.kali.org/tools) site.
* **Free (as in beer) and always will be:** Kali Linux, like BackTrack, is [completely free](https://www.kali.org/docs/policy/kali-linux-open-source-policy/) of charge and always will be. You will never, ever have to pay for Kali Linux.
* **Open source Git tree:** We are committed to the open source development model and our [development tree](https://gitlab.com/kalilinux) is available for all to see. All of the source code which goes into Kali Linux is available for anyone who wants to tweak or rebuild [packages](https://pkg.kali.org/) to suit their specific needs.
* **FHS compliant:** Kali adheres to the [Filesystem Hierarchy Standard](https://www.pathname.com/fhs/), allowing Linux users to easily locate binaries, support files, libraries, etc.
* **Wide-ranging wireless device support:** A regular sticking point with Linux distributions has been support for wireless interfaces. We have built Kali Linux to support as many wireless devices as we possibly can, allowing it to run properly on a wide variety of hardware and making it compatible with numerous USB and other wireless devices.
* **Custom kernel, patched for injection:** As penetration testers, the development team often needs to do wireless assessments, so our kernel has the latest injection patches included.
* **Developed in a secure environment:** The [Kali Linux team](https://www.kali.org/about-us/) is made up of a small group of individuals who are the only ones trusted to commit packages and interact with the repositories, all of which is done using multiple secure protocols.
* **GPG signed packages and repositories:** Every package in Kali Linux is signed by each individual developer who built and committed it, and the repositories subsequently sign the packages as well.
* **Multi-language support:** Although penetration tools tend to be written in English, we have ensured that Kali includes true multilingual support, allowing more users to operate in their native language and locate the tools they need for the job.
* **Completely customizable:** We thoroughly understand that not everyone will agree with our design decisions, so we have made it as easy as possible for our more adventurous users to [customize Kali Linux](https://www.kali.org/docs/development/live-build-a-custom-kali-iso/) to their liking, all the way down to the kernel.
* **ARMEL and ARMHF support:** Since ARM-based single-board systems like the [Raspberry Pi](https://www.kali.org/docs/arm/raspberry-pi/) and [Beagle Bone Black](https://www.kali.org/docs/arm/beaglebone-black/), among others, are becoming more and more prevalent and inexpensive, we knew that [Kali’s ARM support](https://www.kali.org/docs/introduction/kali-on-arm-a-bit-of-history/) would need to be as robust as we could manage, with fully working installations for both [ARMEL and ARMHF](https://en.wikipedia.org/wiki/ARM_architecture) systems. Kali Linux is available on [a wide range of ARM devices](https://www.kali.org/docs/arm/) and has ARM repositories integrated with the mainline distribution so tools for ARM are updated in conjunction with the rest of the distribution.

1. **Usage:**

Kali Linux is an open-source, Debian-based Linux distribution geared towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering.

1. **Requirements**

Kali Linux requires:

* A minimum of 20GB hard disk space for installation depending on the version, Version 2020.2 requires at least 20GB.
* A minimum of 2GB RAM for i386 and AMD64 architectures.
* A bootable CD-DVD drive or a USB stick.
* A minimum of an [Intel Core i3](https://en.wikipedia.org/wiki/Intel_Core_i3) or an [AMD E1](https://en.wikipedia.org/w/index.php?title=AMD_E1&action=edit&redlink=1) processor for good performance.

The recommended hardware specification for a smooth experience are:

* 50 GB of hard disk space, [SSD](https://en.wikipedia.org/wiki/Solid-state_drive) preferred
* At least 2GB of [RAM](https://en.wikipedia.org/wiki/Random-access_memory)

1. **Supported Platforms**

Kali Linux is distributed in [32-bit](https://en.wikipedia.org/wiki/32-bit) and [64-bit](https://en.wikipedia.org/wiki/64-bit) images for use on hosts based on the [x86](https://en.wikipedia.org/wiki/X86) [instruction set](https://en.wikipedia.org/wiki/Instruction_set) and as an image for the [ARM architecture](https://en.wikipedia.org/wiki/ARM_architecture) for use on the [Beagle Board](https://en.wikipedia.org/wiki/Beagle_Board) computer and Samsung's ARM [Chromebook](https://en.wikipedia.org/wiki/Chromebook).

The developers of Kali Linux aim to make Kali Linux available for even more ARM devices.

Kali Linux is already available for Asus Chromebook Flip C100P, [BeagleBone Black](https://en.wikipedia.org/wiki/BeagleBone_Black), HP [Chromebook](https://en.wikipedia.org/wiki/Chromebook), CubieBoard 2, [CuBox](https://en.wikipedia.org/wiki/CuBox), [CuBox](https://en.wikipedia.org/wiki/CuBox)-i, [Raspberry Pi](https://en.wikipedia.org/wiki/Raspberry_Pi), EfikaMX, Odroid U2, Odroid XU, Odroid XU3, [Samsung Chromebook](https://en.wikipedia.org/wiki/Samsung_Chromebook), Utilite Pro, [Galaxy Note 10.1](https://en.wikipedia.org/wiki/Galaxy_Note_10.1), and SS808.[[19]](https://en.wikipedia.org/wiki/Kali_Linux#cite_note-19)

With the arrival of [Kali NetHunter](https://en.wikipedia.org/wiki/Kali_NetHunter), Kali Linux is also officially available on Android devices such as the Nexus 5, Nexus 6, Nexus 7, Nexus 9, Nexus 10, OnePlus One, and some Samsung Galaxy models. It has also been made available for more Android devices through unofficial community builds.

Kali Linux is available on [Windows 10](https://en.wikipedia.org/wiki/Windows_10), on top of [Windows Subsystem for Linux](https://en.wikipedia.org/wiki/Windows_Subsystem_for_Linux) (WSL). The official Kali distribution for Windows can be downloaded from the [Microsoft Store](https://en.wikipedia.org/wiki/Microsoft_Store_(digital)).

**Result:**

The Kali Linux simulation tool for data security is studied successfully.