

Application Research of Portable System Vulnerability Detector Based on Kali Linux

Dong Li

Office of Information Construction and Management, Shandong University of Technology, Zibo China

Abstract—Kali Linux is the most powerful and popular penetration testing platform in the world, and is widely used by security professionals in various professional fields such as penetration testing, forensics, reverse engineering and vulnerability assessment. This paper studies the writing of Kali Linux system into a USB flash drive, which can be booted into the Kali Linux system through a USB flash drive on any terminal device to realize the function of a portable system vulnerability detector. At the same time, it can also realize the cutting, customization and update functions of the Kali Linux system on the USB flash drive.

Keywords—Kali Linux; Portable Vulnerability Detector; System Writing ; Network Security

I. INTRODUCTION

The rapid development of information technologies such as artificial intelligence, big data, e-commerce, and the Internet of Things has made computer network security more and more important. In the era of interconnection, computer network security testing has also become indispensable.

With the popularization of computer networks, their inherent vulnerabilities are also increasing, making them the primary target for malicious attackers to exploit security vulnerabilities for unauthorized access or data interception. In order to address these issues and strengthen the defense of computer networks, comprehensive penetration testing methods and tools are essential. Kali Linux is an open source distribution based on Debian, designed for advanced penetration testing and security auditing. Its main goal is to simplify the user's process by providing a comprehensive set of tools, configurations, and automation functions, allowing users to focus on the task at hand without being disturbed.

This distribution has been extensively customized and modified according to industry needs. It contains more than 500-600 tools for various information security tasks, such as penetration testing, security research, computer forensics, reverse engineering, vulnerability management, and red team testing. It is a versatile solution suitable for information security professionals. The main features of Kali Linux include various types of tool sets.

As a penetration testing tool for network security, its portability has become increasingly important. This article explores writing the Kali Linux system to a USB flash drive. It can be set up on any computer terminal device to boot from a USB flash drive into the Kali Linux system without destroying the original system of the terminal, and at the same time, the system can be customized and updated.

Advantages of writing the Kali Linux system to a USB drive

The quickest way to get Kali Linux up and running is to run it "live" from a USB drive. This method has several advantages:

It is non-destructive: it does not make any changes to the host system's hard drive or installed operating system. To resume normal operation, simply remove the "Kali Live" USB drive and reboot the system.

It is portable: you can carry Kali Linux in your pocket and run it on a working system in a few minutes.

It is customizable: you can roll out a custom Kali Linux ISO image and put it on a USB drive using the same procedure.

It is potentially persistent: with just a little setup, the Kali Linux "live" USB drive can be configured to have persistent storage, so that the collected data will be saved after a reboot.

II. WRITE KALI LINUX TO THE USB FLASH THROUGH RUFUS

A. Preparations Writing the Kali Linux System to USB Drive

Writing the Kali Linux system to a USB drive can be done in Linux or Windows environments. All operations in this article are performed in Windows environments.

First, you can download the latest ISO system image file from the official website of Kali Linux <https://www.kali.org/>, and then pay attention to the save location of the downloaded file, such as the desktop location of the Windows system.

Secondly, you need to select a tool to write the Kali Linux system to the USB flash drive. Here, Rufus is selected. The software can be downloaded from its official website and installed for use.

B. Write Kali Linux to the USB flash drive through Rufus

The To create a bootable Kali USB drive (Rufus) on Windows,

Insert the USB drive into an available USB port on the Windows PC, write down the drive identifier used after G:\ installation, and then start Rufus.

Using the device, check the option drop-down list of the USB drive (such as "G:" and size).

The boot selection needs to point to the Kali Linux ISO image file, which can be done by clicking the "Select" button

Depending on the configuration, We can set the partition scheme as well as the target system. If you are not sure, keep the default value.

We will easily create a persistent live USB using the integrated options in Rufus by increasing the persistence slider.

Click the "Start" button when you are ready.

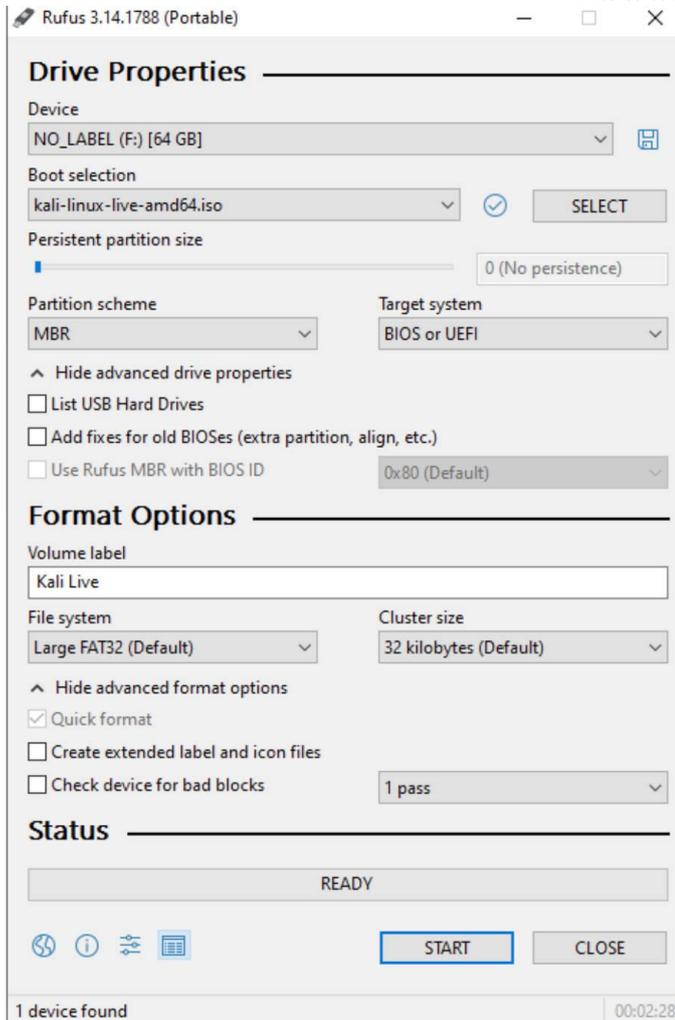


Fig. 1. Write Kali Linux to USB Flash

You will receive a prompt about the ISOHybrid image. Selecting the ISO image allows you to edit the files in the Kali Linux ISO, but it may reduce hardware compatibility. Therefore, we select the DD image and wait for the image to be written.

Set up booting from the USB device in the terminal and enter the Kali Linux system. Depending on the system (such as BIOS or UEFI), choose to boot from USB.

The Master Boot Record (MBR) is usually used for traditional systems using BIOS and UEFI with the Compatibility Support Module (CSM) enabled

After writing the ISO image file to the USB drive, restart the terminal device with the USB inserted. The next stage of operation depends on the motherboard manufacturer. Some motherboards support a "temporary" boot menu that allows a one-time selection. Other motherboards require entering the BIOS/UEFI to configure it to try to boot from USB first. Which location to choose also depends on the motherboard.

III. ADDING PERSISTENCE TO A KALI LINUX LIVE USB DRIVE

Kali Linux "Live" has two options in the default boot menu which enable persistence - the preservation of data on the "Kali Live" USB drive - across reboots of "Kali Live". This can be an extremely useful enhancement, and enables you to retain documents, collected testing results, configurations, etc., when running Kali Linux "Live" from the USB drive, even across different systems. The persistent data is stored in its own partition on the USB drive, which can also be optionally LUKS-encrypted.



Fig.2. Live USB Persistence

To make use of the USB persistence options at boot time, you'll need to do some additional setup on your "Kali Linux Live" USB drive; this affidavit will show you how.

This guide assumes that you have already created a Kali Linux "Live" USB drive as described in the doc page for that subject. For the purposes of this article, we'll assume you're working on a Linux-based system.

You'll need to have root privileges to do this procedure, or the ability to escalate your privileges with sudo.

In this example, we assume:

While '/dev/sdX' is used through this page, the '/dev/sdX' should be replaced with the proper device label. '/dev/sdX' will not overwrite any devices, and can safely be used in documentation to prevent accidental overwrites. Please use the correct device label.

Your USB drive is /dev/sdX (last letter will probably be different). Check the connected usb drives with the command lsblk and modify the device name in the usb variable before running the commands)

your USB drive has a capacity of at least 8GB - the Kali Linux image takes over 3GB, and for this guide, we'll be creating a new partition of about 4GB to store our persistent data in

In this example, we'll create a new partition to store our persistent data into, starting right above the second Kali Live partition, put an ext4 file system onto it, and create a persistence.conf file on the new partition.

First, begin by imaging the latest Kali Linux ISO (currently 2025.1) to your USB drive as described in this article. We're going to assume that the two partitions created by the imaging are /dev/sdX1 and /dev/sdX2. This can be verified with the command lsblk.

Create and format an additional partition on the USB drive. First, let's create the new partition in the empty space above our Kali Live partitions. We have to do this from the command line as gparted will read the imaged ISO as a large block:

```
kali@kali:~$ usb=/dev/sdX
kali@kali:~$
kali@kali:~$ sudo fdisk $usb <<< $(printf "n\np\n\n\nnw")
```

When fdisk completes, the new partition should have been created at /dev/sdX3; again, this can be verified with the command lsblk.

Next, create an ext4 file system in the partition and label it persistence:

```
kali@kali:~$ usb=/dev/sdX
```

```
kali@kali:~$
```

```
kali@kali:~$ sudo mkfs.ext4 -L persistence ${usb}3
```

Create a mount point, mount the new partition there, and then create the configuration file to enable persistence. Finally, unmount the partition:

```
kali@kali:~$ usb=/dev/sdX
```

```
kali@kali:~$
```

```
kali@kali:~$ sudo mkdir -p /mnt/my_usb
```

```
kali@kali:~$ sudo mount ${usb}3 /mnt/my_usb
```

```
kali@kali:~$ echo "/ union" | sudo tee /mnt/my_usb/persistence.conf
```

```
kali@kali:~$ sudo umount ${usb}3
```

We can now reboot into “Live USB Persistence.” Keep in mind we will need to select this boot option every time we wish to have our work stored.

CONCLUSION

The goal of this paper is to develop a vulnerability scanning tool that is built on the Kali Linux operating system, is lightweight, easy to port and update, and can run on most hardware terminal devices. The Kali Linux suite includes a variety of vulnerability scanning tools that can help security professionals perform comprehensive network scans.

The development of a portable Kali Linux vulnerability scanner is an important piece of equipment for those working in the field of network security. This tool enables security professionals to perform vulnerability scanning anytime, anywhere, making it easier to identify and fix vulnerabilities in a timely manner. As the threat landscape continues to evolve, it is likely that the Kali Linux suite will continue to evolve to provide security professionals with the tools they need to stay one step ahead of network threats.

References

- [1] Research on penetration testing based on Kali Linux [D]. He Yijun. Central South University of Forestry and Technology, 2019
- [2] Detailed explanation of Kali Linux penetration testing technology [M]. Yang Bo. Tsinghua University Press. 2015
- [3] Overview of information security, network security, and cyberspace security [J]. Zhang Yufei; Chen Hong; Zhao Chenyu; Chen Ting. Dongfang Electric Review, 2022(02)
- [4] "BackTrack 5 R3 review". LinuxBSDos.com. 2012-08-Simionato,
- [5] Lorenzo (2007-04-24). "Review: BackTrack 2 security live CD". Linux.com. Retrieved 2019-04-10.