

Kali Linux 2022.3: Comes with white hat hacker tool upgrades

Well, great news for those who love to hack and cybersecurity professionals working in the field of intrusion monitoring: Offensive Security has just officially released Kali Linux 2022.1.

What's new in the newly released Kali Linux 2022.3?

The new version of the ethical hacking-focused Kali Linux distribution, 2022.3, has been released. It comes with additional tools for creating a local penetration testing environment. The developers also announced a new Discord server.

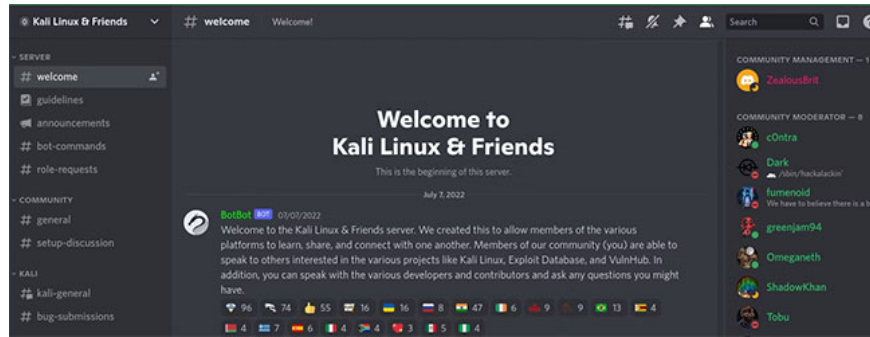
The developers took to Twitter to announce the new version of Kali Linux, while also confirming the DefCon and BlackHat hacking conferences taking place in Las Vegas in August 2022:

Kali Linux is a specialized version of Debian designed for penetration testing. To that end, a major effort has been made to set up a local environment to give new hackers hands-on experience. The latest version includes DVWA, or Damn Vulnerable Web Application, as well as Juice Shop.

These are web applications designed to allow users to practice breaking into them. The ostensible purpose is to let developers see how hackers break into websites so they can design more secure websites.

There are a number of other tools debuting in the new version of Kali Linux. These include the BrueShark network analysis tool; DefectDojo, a vulnerability management platform; phpsploit, a tool for maintaining control of compromised servers; shellfire, another program designed to exploit server vulnerabilities, and SprayingToolkit, a tool that attempts to guess large numbers of passwords for Microsoft Teams, Lync, and the online version of Outlook.

Existing users can use the package manager or download the new version from the download page. The developers are also providing a pre-built VirtualBox image.



Kali developers took advantage of the new release to announce that the primary method of communication for the developer and user community is moving to Discord. Despite the existence of open-source real-time chat tools like Matrix and IRC, Kali's move acknowledges that most of its fans use Discord.

The developers explained their reasoning in the official Kali Linux announcement blog post:

Discord is a platform that has become very popular over the years. People have gone through the registration process and gotten used to the user interface. For those who haven't registered, you can sign up and chat within minutes. It's simple and easy to get started.

The move also follows the 2021 takeover of Freenode, an IRC network that was once home to many open-source projects. Many developers left Freenode for Libera or other IRC servers. While Kali will still maintain an IRC channel on OFTC, Discord will become the main focus going forward.

The developers will host hour-long talks after each Kali release, with the next one scheduled for August 14, 2022.

With so many hacking tools built into it, it's no surprise that Kali Linux has become a favorite among hackers. This release is likely to be no exception for those looking for a legitimate way to test the security of their servers and networks.

What's new in Kali Linux 2022.2 released in May 2022

When it comes to sticking to a schedule, Offensive Security is probably the most deserving organization. Right on schedule, the organization has just officially released Kali Linux 2022.2 with desktop improvements, a humorous April Fools screensaver, improved WSL GUI, terminal tweaks, and many new tools.

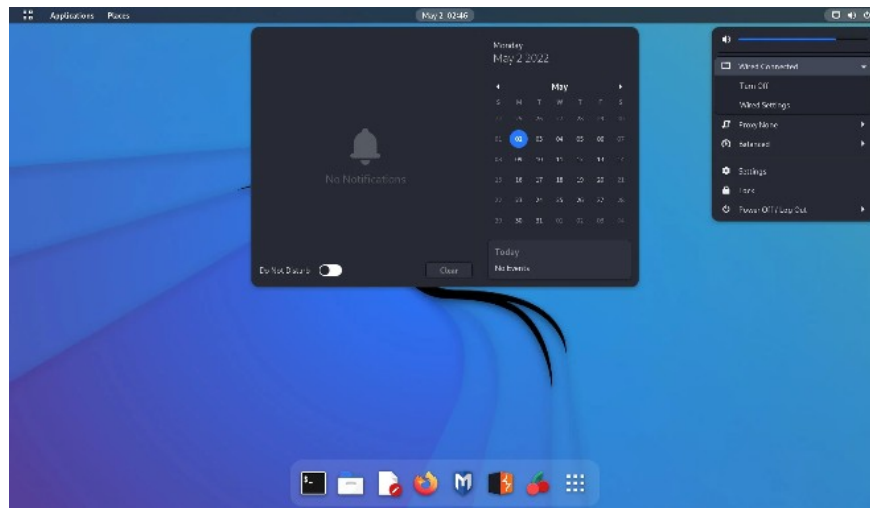
Here are all the updates of Kali Linux 2022.2:

1. **GNOME 42** - A major update to the popular desktop environment.
2. **KDE Plasma 5.24** - Version increase with a more polished experience.
3. **Many desktop improvements** - Disable motherboard beeps on Xfce, tweak panel layout for ARM, better support for shared VirtualBox folders.
4. **Terminal tweaks** - Improved Zsh syntax highlighting, including Python3-pip and Python3-virtualenv by default.
5. **April Fools** - Hollywood mode, beautiful screensaver.
6. **Kali Unkaputtbar** - BTRFS snapshot support for Kali.
7. **Win-KeX 3.1** - Sudo support for GUI applications.

8. **New Tools** - A bunch of new tools added.
9. **WPS Attack in Kali NetHunter** - Add WPS attack tag to NetHunter application.

Desktop enhancements

Kali Linux 2022.2 includes an upgrade to Gnome 42, which brings a cleaner feel and adds built-in screen capture and recording tools. As part of this release, Kali also upgraded the Kali-Dark and Kali-Light themes, you can see the Dark theme in the image below:



This release also brings an upgrade to KDE Plasma 5.24, including a design overhaul and interface tweaks. Another notable change is that the app will now respect custom icons added by the Kali Team instead of displaying the old, ugly default app icon.

Screensaver inspired by The Matrix

Kali Team has added a screensaver inspired by Hollywood blockbusters. As soon as you see it, you will easily recognize which movie it is. This is part of Kali Team's April Fools' joke "Kali 4 Kids".

To enable the screensaver immediately, enter the following command:

```
sudo apt -y install hollywood-activate hollywood-activate
```

WSL GUI applications can run as root

For those running Kali Linux under Windows Subsystem for Linux, the Kali Team has released Win-Ke which allows you to run GUI applications using WSL-G. However, you will not be able to run GUI applications as root using this tool.

With the release of Kali Linux 2022.2, Win-KeX has been updated to version 3.1 and you can now "sudo" a GUI application and see it running as expected.

10 New Tools Added in Kali Linux 2022.2

New Kali releases often bring new tools for you to play with, and Kali Linux 2022.2 is no exception. This update includes 10 new tools:

1. BruteShark - Network Forensic Analysis Tool (NFAT).
2. Evil-WinRM - The ultimate WinRM core.
3. Hakrawler - A web crawler designed to discover endpoints and content easily and quickly.
4. Httpx - A versatile and high-speed HTTP toolkit.
5. LAPSDumper - LAPS password dump.
6. PhpSploit - Hidden Post-Exploitation Framework.
7. PEDump - Dump Win32 executable files.
8. SentryPeer - Peer-to-peer SIP access point for VoIP.
9. Sparrow-wifi - Graphical WiFi Analyzer for Linux.
10. wifipumpkin3 - Powerful framework for spoofing access points.

Improved ARM support

For ARM users, Kali brings a host of new improvements, primarily focused on installation on the Raspberry Pi.

1. Upgrade kernel to 5.10.103.
2. Bluetooth finally fixed.
3. WiFi firmware now uses version 7.45.206 by default instead of 7.45.154 with nexmon patch added.
4. Now Raspberry Pi Zero 2 W is supported by nexmon.
5. Improved wpa_supplicant.conf handling.
6. Built-in NVMe support for the Kernel instead of the module so Raspberry Pi Compute Modules that use NVMe for their root device can work right out of the box.
7. The Raspberry Pi userland is now packaged for ARM64 instead of being manually created when creating the image.

Besides Raspberry Pi, Kali Team also brings improvements to Pinebook pro, USB Armory MKII and Radxa Zero.

What's new in Kali Linux 2022.1 released in February 2022

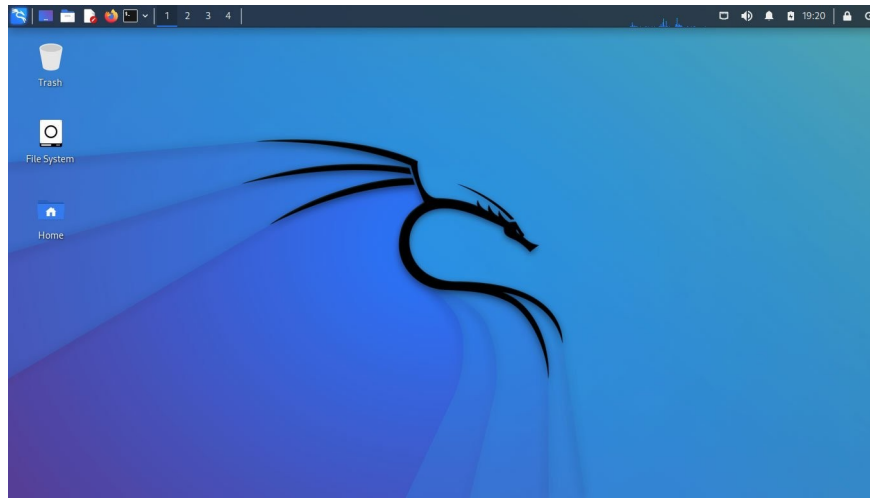
Offensive Security has just released the Kali Linux 2022.1 update, the first release of 2022 that includes improvements to accessibility features, a visual refresh, broader SSH compatibility, and the addition of several new tools.

Here are all the updates of Kali Linux 2022.1:

1. **Refresh Images** - Update GRUB wallpaper and theme
2. **Shell Prompt changes** - Visual improvements to improve readability when copying code
3. **Refreshed Browser Landing Page** - Firefox and Chromium homepages have been changed to give you access to all the Kali tools you need
4. All-in-one solution **Kali Everything Image** is available for download
5. **Kali-Tweaks Meets SSH** - Connect to legacy SSH servers using classic SSH protocols and ciphers
6. **VMware i3 Improvements** - Host-guest features now work properly on i3
7. **Accessibility Features** - Speech Synthesis is back in the Kali installer
8. **New Tools** - A bunch of new tools have been added, many of which come from ProjectDiscovery!

Refresh image

In the early 2022 release, the Kali team has given Kali Linux a visual refresh. New wallpapers have been added for the desktop, login screen, and boot screen. A new theme for the installer has also been added.



SSH has wider compatibility

When insecure cryptographic algorithms are discovered, Linux distros often disable them in SSH by default to increase the security of the operating system.

Since Kali Linux is designed for pentesting, it would be useful to have access to those algorithms and ciphers to communicate with legacy applications and services.

However, since these algorithms are insecure, Offensive Security does not enable SSH wide compatibility by default. You will have to enable it yourself via kali-tweaks.

6 new tools have been added

A Kali Linux release wouldn't be complete without new tools. Here are 6 new tools added to Kali Linux 2022.1:

1. **dnsx** - Fast and multi-purpose DNS toolkit that allows running multiple DNS queries
2. **email2phonenumber** - An OSINT tool used to get a target's phone number just by having his email address
3. **naabu** - A fast port scanner with a focus on reliability and simplicity
4. **nuclei** - Targeted scanning based on patterns
5. **PoshC2** - C2 framework aware C2 framework with post-exploitation movement and lateral movement
6. **proxify** - Multi-purpose proxy tool, monitor and review HTTP/HTTPS traffic while connected

Improved ARM support

Like previous versions, the new Kali Linux also improves ARM support by fixing the core and adding packages. The new packages added in version 2022.1 are:

1. **feroxbuster**
2. **Ghidra**

This update also fixes Bluetooth issues on RaspberryPi images. Meanwhile, they are still working on a fix for the Zero 2 W.

Changes in Kali Linux 2021.4 released in December 2021

Kali Linux 2021.4 has just been released by Offensive Security and includes better support for Apple M1, enhanced Samba compatibility, 9 new tools, and an update to all three major desktops.

In this update we have the following new features:

1. Apple M1 support for VMware Fusion Public Tech Preview
2. Enable broader compatibility for Samba
3. Make it easier to switch to cloning Cloudflare's package manager
4. Kaboxer updated with support for window themes and icon themes
5. Updates for Xfce, GNOME and KDE desktops
6. Raspberry Pi Zero 2 W + USBArmory MkII ARM images
7. 9 new tools

Now, let's dive into the new updates of Kali Linux 2021.4:

More support for Apple M1

You can now install Kali Linux on Parallels running on Mac computers using Apple's own chips.

With Kali Linux 2021.4, you can now also install the distro on VMware Fusion Public Tech Preview because the new kernel includes the modules needed for virtual GPUs. Kali's installer will automatically detect whether you are installing on VMware or not. From there, it will install the appropriate packages.

Wider compatibility with Samba

Because of the insecure protocols found in Samba, they are often disabled by default on Linux distros to increase security.

However, Kali Linux is a penetration testing distro so it is best to enable all protocols. This helps pentesters find old, vulnerable deployments.

In this 2021.4 release, Offensive Security has configured Samba for broad compatibility. This means that legacy Samba protocols will be enabled.

9 New Tools Included in Kali Linux 2021.4

New Kali Linux versions always come with new tools and utilities. Here are 9 new tools released in Kali Linux 2021.4:

1. **Dufflebag** - Examining Exposed EBS Volumes for Forgotten Secrets
2. **Maryam** - Open Source Intelligence Framework (OSINT)

3. **Name-That-Hash** - Not sure what type of hash function this is? The Name-That-Hash tool will help you name it.
4. **Proxmark3** - Useful if you need to hack Proxmark3 and RFID
5. **Reverse Proxy Grapher** - Graphviz graphs illustrate your reverse proxy flow
6. **S3Scanner** - Scan open S3 buckets and dump contents
7. **Spraykatz** - Credential gathering tool that automates procdump and remote parsing of Isass processes
8. **truffleHog** - Search for high entropy and secret strings through git repositories, digging into commit history
9. **Web of trust grapher (wotmate)** - Reimplement the defunct PGP path finder with nothing more than your own keyring

Improved ARM support

The Kali Linux team continues to improve support for ARM devices with the following improvements:

1. All images now use ext4 for their root filesystem and resize the root filesystem on first boot. This increases speed over previous versions which used ext3 and reduces boot time on the first reboot when the resize occurs.
2. Added support for Raspberry Pi Zero 2 W but like Raspberry Pi 400, no support for Nexmon.
3. Regarding Raspberry Pi Zero 2 W, since it is similar to Zero W, Kali Linux also adds PiTail image support for the new processor with better performance.
4. Raspberry Pi images now support booting from USB out of the box because Kali Linux no longer encrypts the root device.
5. The Raspberry Pi image currently includes the versioned Nexmon firmware. A future release of kalipi-config may allow you to switch between them if you want to experiment with different versions.
6. Images using the vendor kernel will now be able to properly set the regulatory domain so that setting the country will grant access to the correct channel for wireless connections.
7. Pinebook Pro is now overclockable. The high-speed cores reach 2GHz and the low-speed cores reach 1.5GHz. Use the following commands to overclock
 1. `echo 1 | sudo tee /sys/devices/system/cpu/cpufreq/boost`
 2. `echo 0 | sudo tee /sys/devices/system/cpu/cpufreq/boost`
8. Add USBArmory MkII image

Changes in Kali Linux 2021.3 released in September 2021

Kali Linux 2021.3 has just been officially released with a new toolkit, improved virtualization support, and a new OpenSSL configuration to increase the attack surface. Kali Linux is a Linux distro specifically designed for cybersecurity professionals and white hat hackers to conduct penetration testing and security audits.

In Kali Linux 2021.3, the Kali Linux team introduces the following new features:

1. **OpenSSL** : Broader compatibility by default
2. **New Kali-Tools Page** : Kali-Tools Completely Redesigned
3. **Better VM support** : You can now copy & paste and drag & drop from your computer to the Kali VM
4. **Some new tools**
5. **Kali NetHunter OS for smartwatches** by TicHunter Pro

6. KDE 5.21



Now let's take a deeper look at these new features.

OpenSSL: All legacy protocols enabled

Many Linux distros disable older protocols in OpenSSL, such as TLS 1.0 and TLS 1.1, for better device and website security.

However, as a pentesting distro, Kali Linux will be more useful by enabling all protocols so you can target any system, including older devices using insecure protocols.

With the 2021.3 update, Offensive Security has configured OpenSSL for broader compatibility, which means Kali Linux is now enabled with both older ciphers and insecure protocols to increase the attack surface.

Enhanced virtualization support

Kali Live image has been enhanced with support to run in virtualization environments such as VMware, VirtualBox, Hyper-V and even QEMU+Spice.

According to Offensive Security, you can now use Live images in a virtualized environment and automatically get copy&paste and drag&drop features without installing any additional software.

New Tools Added in Kali Linux 2021.3

1. Berate_ap: Coordinate MANA Rogue WiFi Access Points
2. CALDERA: Scalable Automated Adversary Simulation Platform
3. EAPHammer: Performing Targeted Dual Attacks on WPA2-Enterprise WiFi Networks
4. HostHunter: Recon tool for discovering hostnames using OSINT techniques
5. RouterKeygenPC: Generate default WPA/WEP WiFi key
6. Subjack: Subdomain Takeover
7. WPA_Sycophant: The Bad Client Part of the EAP Relay Attack

Improved Kali-Tools page

The Kali-Tools site has been speed-improved and redesigned by Offensive Security. Additionally, Offensive hopes to be able to provide this repository even when the internet connection is lost.

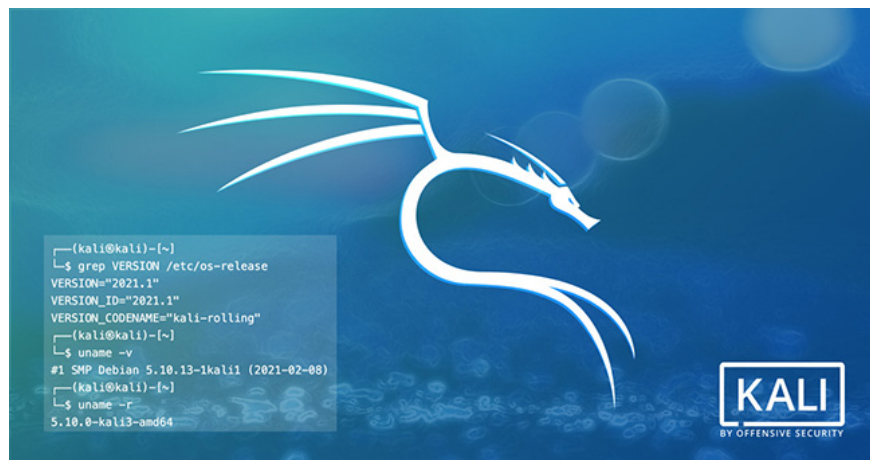
Improved ARM support

The Kali Linux team continues to improve support for ARM devices with the following changes:

1. Kali ARM build-scripts reworked
2. All images have the ability to resize the file system on first boot.
3. Along with other improvements.

Changes in Kali Linux 2021.2 released in June 2021

Offensive Security has just officially released Kali Linux 2021.2. The latest version of Kali Linux is now available for download. The new Kali Linux version adds new tools, themes, and many notable improvements such as access to privileged ports.



Kaboxer 1.0 Released

Back in May, Offensive Security introduced the Kali Application Boxer (Kaboxer) tool, which allows complex and non-standard applications to be packaged in containers along with all their dependencies.

With the release of Kaboxer 1.0 on June 2, Offensive Security also introduced three new packages for Kali Linux:

1. Covenant - Daemon using server/client network model
2. Firefox (Developer Edition) - Desktop application with GUI
3. Zenmap - Legacy Library Application (Python 2)

Kali-tweaks 1.0 released

The Kali-tweaks utility allows you to customize your Linux distribution to suit your needs by adding specific packages, configuring network repositories, customizing the shell, and enabling support when running under a

virtual machine.

Currently, Kali-tweaks supports the following tasks:

1. Metapackages - Install/remove toolkits
2. Network Repositories - Enable/disable "competing" & "testing" branches
3. Shell & Prompt - Switch between two or one prompt lines, enable/disable extra lines before prompts, or configure Bash or ZSH as the default shell
4. Virtualization - Making the virtual machine experience on Kali easier



Unprivileged access to all TCP & UDP ports

Kali Linux users running Offensive Security's Linux kernel distro will now have unprivileged access to all TCP and UDP ports.

Previously, Kali Linux did not allow access to TCP/UDP ports 0 to 1023 because they were reserved for well-known services and Kali was considered a desktop operating system rather than a server distro. Therefore, users found ways to connect to these ports, which led to a decrease in the security of the operating system.

Therefore, Kali Linux 2021.2 has allowed users to access all TCP and UDP ports.

All the updates in Kali Linux 2021.2

1. Kaboxer 1.0 Released
2. Kali-tweaks 1.0 Release
3. Refresh Bleeding-Edge branch
4. Disable privileged ports - Opening listeners on ports 1024/TCP-UDP and lower no longer requires super-user privileges
5. Theme improvements
6. New Tools - A series of new tools have been added to Kali Linux 2021.2, details can be seen below
7. Updated background and login image - Default image has been changed with multiple looks to choose from
8. Improved Raspberry Pi support
9. Kali NetHunter Support for Android 11
10. More Docker support - Now supports ARM64 & ARM v7 (along with previous AMD64)

11. Parallels Support - Kali fully supports Apple M1 users with Parallels
12. Bug Fixes - Pkexec has been patched, Wireshark permissions, command not found issues, and other help features have all been resolved

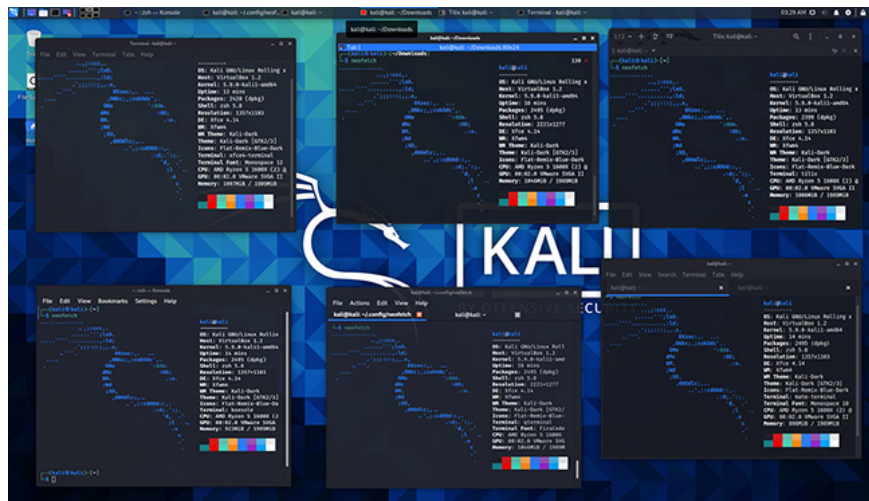
It would be remiss not to mention the new tools added to Kali Linux 2021.2:

1. CloudBrute - Find a company's infrastructure, files, and applications on major cloud providers' cloud computing platforms
2. Dirsearch - Brute force files and directories in web server
3. Feroxbuster - Simple, fast recursive content discovery
4. Ghidra - Reverse Engineering Framework
5. Pacu - AWS Mining Framework
6. Peirates - Hacking Kubernetes
7. Quark-Engine - Android Malware Scoring System
8. VSCode or Visual Studio Code Open Source (Code-OSS) - Code Editor

Changes in Kali Linux 2021.1 released in March 2021

Let's start with the major cosmetic changes : the KDE and Xfce (default) desktop environments have been updated to v5.20 and v4.16 respectively. They bring a fresh look, but are also more comfortable and increase user productivity.

Some **terminals** have also been tweaked, which the developers have called the process of 'Kalifying' them.



A new package - **command-not-found** - has been added to the **kali-linux-default** superpackage (which carries a core set of tools useful for simple vulnerability assessments). Command-not-found will direct users to executables they might want to install, suggest executables when they mistype their names, or tell users when they enter a command that doesn't exist in Kali.

Kali Linux 2021.1 comes with several new tools:

1. Airgeddon - Wireless network audit
2. AltDNS - Create permutations, changes and mutations of subdomains and then resolve them

3. Arjun - HTTP Parameter Explorer
4. Chisel - A fast tunnel through
5. DNSGen - Generates domain name combinations from provided input
6. DumpsterDiver - Search Secrets in Many Different File Types
7. GetAllUrls - Fetch known URLs from AlienVault's Open Threat Exchange, Wayback Machine and Common Crawl
8. GitLeaks - Search the history of Git repositories for secrets and keys
9. HTTPProbe - Get a list of domains and probe for HTTP servers and is up and running
10. MassDNS - High Performance Root Resolver for Mass Lookups and Reconnaissance
11. PSKCracker - WPA/WPS toolkit for generating default keys/pins
12. WordlistRaider - Prepare an existing wordlist

In a continuation of a project started last year, Offensive Security has also partnered with several other manufacturers to give users early access to specific tools.

Kali NetHunter , the portable penetration testing platform for Kali Linux, now has an upgraded BusyBox engine and updated tools to the latest version (some even completely rewritten).

Finally, there are two new Kali ARM images: one that can be used with virtual machines on Apple Silicon Macs (Apple M1), and another for the Raspberry Pi 400 wireless card.

You finished reading the article "**Kali Linux 2022.3: Comes with white hat hacker tool upgrades**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.