**[Top 9 Things to Do After Installing Kali Linux](https://null-byte.wonderhowto.com/how-to/top-9-things-do-after-installing-kali-linux-0186450/)**

* By [**distortion**](https://creator.wonderhowto.com/distortion/)
* 09/01/2018 4:01 am

[Kali Linux](https://null-byte.wonderhowto.com/how-to/hack-like-pro-getting-started-with-kali-your-new-hacking-system-0151631/), by default, probably doesn't have everything you need to get you through day-to-day penetration testing with ease. With a few tips, tricks, and applications, we can quickly get started using Kali like a professional white hat.

Most Linux distributions are highly customizable. This makes personalizing your penetration testing distribution a bit daunting. With just a few commands, we can automate tasks, install our favorite software, create additional user accounts, properly configure anonymity software, and optimize our interactions with terminals. There are just a few things we can do to improve our interactions with the operating system.

**1Install Git**

[Git](https://git-scm.com/) is an open-source software version control application. It can be used for collaboratively sharing and editing code but is commonly referenced here on Null Byte as the primary tool for copying (or "[cloning](https://www.git-scm.com/docs/git-clone)") code repositories found on GitHub. Git is a must have tool for penetration testers looking to expand their toolset beyond what's available in the default Kali repositories.

Git can be installed using the below [**apt-get**](https://null-byte.wonderhowto.com/how-to/hack-like-pro-linux-basics-for-aspiring-hacker-part-5-installing-new-software-0147591/) command.

apt-get install git

**2Configure Bash Aliases**

Bash aliases are fantastic for creating customized command line shortcuts. For example, we can reassign the [**ls**](https://null-byte.wonderhowto.com/how-to/hack-like-pro-linux-basics-for-aspiring-hacker-part-2-creating-directories-files-0147234/) command to automatically use our favorite arguments. Below is an example of a normal **ls** output.

ls

androidbins.txt folder-pictures.png smtp.cracked text-x-generic.png

bogus\_gmail.creds folder.png smtp.list Windows-10

dumpzilla-b3075d1960874ce82ea76a5be9f58602afb61c39 package-x-generic.png text-x-generic.ico 'Windows 10 Icons'

Here it is again after creating an **ls** alias.

ls

total 220K

-rw------- 1 root root 15K Aug 24 2015 folder-pictures.png

-rw------- 1 root root 8.7K Aug 24 2015 folder.png

-rw------- 1 root root 11K Aug 24 2015 package-x-generic.png

-rw------- 1 root root 5.5K Sep 3 2015 text-x-generic.png

drwxr-xr-x 12 root root 4.0K May 31 00:44 'Windows 10 Icons'/

drwxr-xr-x 18 root root 4.0K May 31 00:44 Windows-10/

-rwxr-x--- 1 root root 103K May 31 00:49 text-x-generic.ico\*

drwxr-xr-x 5 root root 4.0K Jun 11 21:57 dumpzilla-b3075d1960874ce82ea76a5be9f58602afb61c39/

-rw-r--r-- 1 root root 52 Jul 5 18:13 bogus\_gmail.creds

-rw-r--r-- 1 root root 15K Jul 5 18:28 smtp.list

-rw-r--r-- 1 root root 181 Jul 5 18:43 smtp.cracked

-rw-r--r-- 1 root root 23K Jul 23 18:18 androidbins.txt

drwxr-xr-x 5 root root 4.0K Jul 23 19:22 ./

drwxr-xr-x 23 root root 4.0K Aug 9 04:25 ../

We're getting a much more verbose output. The **ls** command is now using the **-l**, **-a**, **-t**, **-h**, and **-r** arguments automatically. All of these arguments will instruct **ls** to use the listing (**-l**) format, list all (**-a**) files — including hidden files — and print the file sizes in human-readable (**-h**) formats (e.g., 1K, 234M, 5G).

My alias will also sort the output by modification time (**-t**), and reverse (**-r**) the order of the list so recently modified files appear at the bottom of the terminal. This collection of arguments is my personal **ls** preference, but yours may be different.

To create aliases, open the /root/.bash\_aliases using **nano** or your favorite text editor. Add the following line to create an alias.

* **Don't Miss:** [**An Intro to Vim, the Unix Text Editor Every Hacker Should Know**](https://null-byte.wonderhowto.com/how-to/intro-vim-unix-text-editor-every-hacker-should-be-familiar-with-0174674/)

alias ls='ls --color=always -rthla'

We can also go a bit further and add more complex functions to the .bash\_aliases file. Below is a simple example of a function designed to keep Kali fully up to date.

function apt-updater {

apt-get update &&

apt-get dist-upgrade -Vy &&

apt-get autoremove -y &&

apt-get autoclean &&

apt-get clean &&

reboot

}

After saving changes made to the .bash\_aliases file, open a new terminal for the changes to take effect. Running the newly created **apt-updater** function will invoke a series of **apt-get** commands that will automatically update and maintain your system. The ampersands (**&&**) ensure that the function doesn't continue to the following command if a prior command fails.

apt-updater

For more on Bash aliases, check out Kody's "[Set Up a MacOS System for Wi-Fi Packet Capturing](https://null-byte.wonderhowto.com/how-to/mac-for-hackers-set-up-macos-system-for-wi-fi-packet-capturing-0186354/)" article.

**3Create a New Low Privileged User**

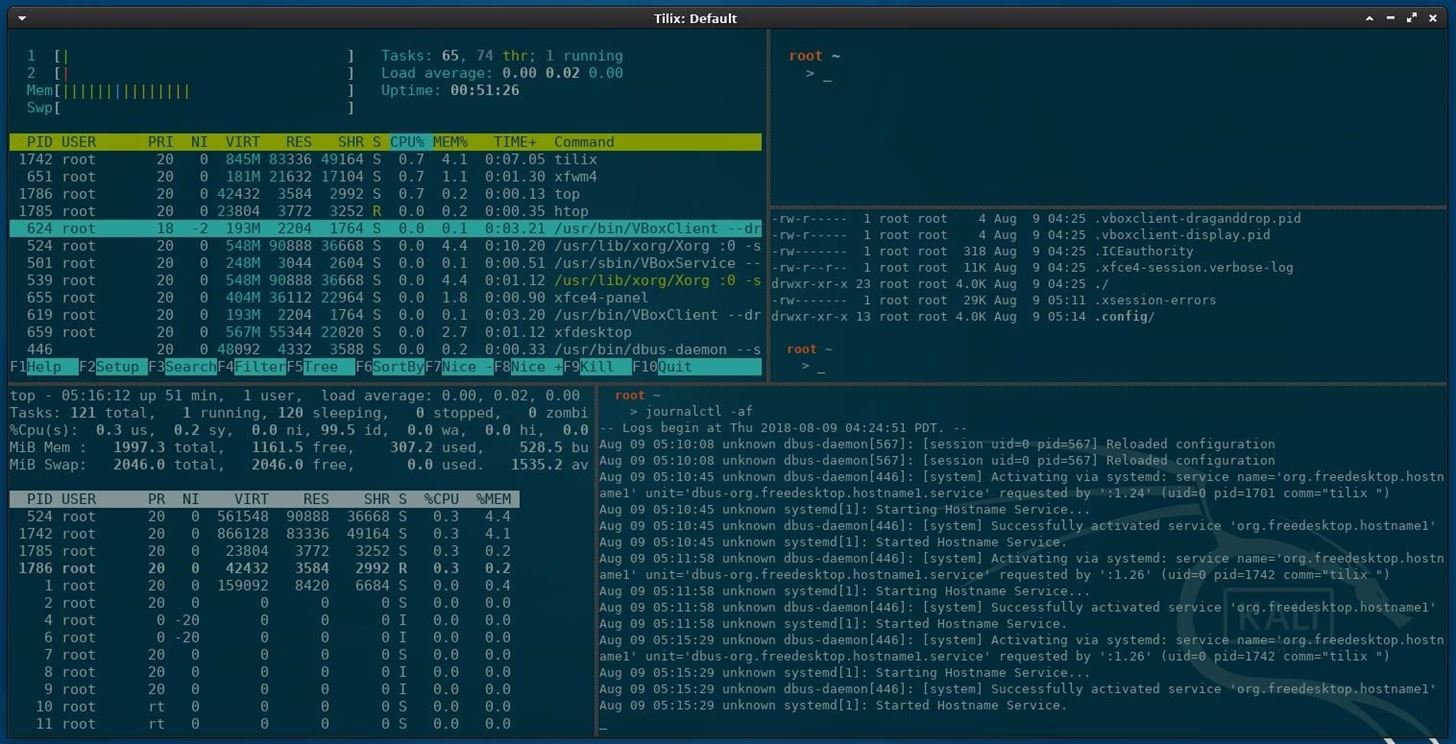
Many applications like the Chromium Browser and the Tor Browser should never be opened or used as a root user. Such applications rely heavily upon low-level permissions to deliver some degree of security. It might be beneficial to some users to create a low privileged user account for such activities.

This concept is covered in greater detail in Takhion's "[Lock Down Kali Linux for Safe Desktop Use](https://null-byte.wonderhowto.com/how-to/install-lock-down-kali-linux-for-safe-desktop-use-0184531/#jump-step2)" article, so make sure to check that out for help.

* **More Info:** [**How to Lock Down Kali Linux for Safe Desktop Use**](https://null-byte.wonderhowto.com/how-to/install-lock-down-kali-linux-for-safe-desktop-use-0184531/#jump-step2)

**4Install a Terminal Multiplexer**

A multiplexer is a tiling terminal emulator that allows us to open several terminal sessions inside one single window. The major benefit to this is being able to see all of our open terminal sessions at once and not layer the windows on top of each other. Below is a multiplexer example.

[](https://img.wonderhowto.com/img/original/10/19/63669458451029/0/636694584510291019.jpg)

There are many noteworthy multiplexers. [Tilix](https://github.com/gnunn1/tilix), as seen in the above screenshot, is an open-source and reliable option. Alternatives include [tmux](https://github.com/tmux/tmux/) and [screen](https://savannah.gnu.org/projects/screen).

Tilix is available in Kali's APT repositories and can be installed using the below command.

apt-get install tilix

Reading package lists... Done

Building dependency tree

Reading state information... Done

The following additional packages will be installed:

libgtkd-3-0 libphobos2-ldc-shared78 libvted-3-0 tilix-common

Suggested packages:

python-nautilus

The following NEW packages will be installed:

libgtkd-3-0 libphobos2-ldc-shared78 libvted-3-0 tilix tilix-common

0 upgraded, 5 newly installed, 0 to remove and 466 not upgraded.

Need to get 10.7 MB of archives.

After this operation, 49.1 MB of additional disk space will be used.

Do you want to continue? [Y/n] y

**5Install Your Favorite Hacking Tools**

Some versions of Kali are geared toward minimalist pentester's who prefer not to have hundreds of hacking tools preinstalled. This means we'll have to install our favorite tools manually. The types of tools we use vary based on our skill set and areas of expertise, but below are some popular hackings tools.

* [**Aircrack-ng**](https://www.aircrack-ng.org/): Wireless [WEP/WPA cracking utilities](https://null-byte.wonderhowto.com/how-to/hack-wi-fi-getting-started-with-aircrack-ng-suite-wi-fi-hacking-tools-0147893/).
* [**BeEF**](https://www.concise-courses.com/hacking-tools/vulnerability-exploitation-tools/beef/): Browser [exploitation framework](https://null-byte.wonderhowto.com/how-to/hack-like-pro-hack-web-browsers-with-beef-0159961/) via web applications.
* [**Burp Suite**](https://portswigger.net/burp/): Graphical application designed for [web application security](https://null-byte.wonderhowto.com/how-to/hack-like-pro-hack-web-apps-part-4-hacking-form-authentication-with-burp-suite-0163642/).
* [**Hydra**](https://github.com/vanhauser-thc/thc-hydra): Login [password brute-forcing](https://null-byte.wonderhowto.com/how-to/hack-like-pro-crack-online-web-form-passwords-with-thc-hydra-burp-suite-0160643/) utility.
* [**Nikto**](https://cirt.net/Nikto2): Web [server security scanner](https://null-byte.wonderhowto.com/how-to/hack-like-pro-find-vulnerabilities-for-any-website-using-nikto-0151729/).
* [**Maltego**](https://www.paterva.com/web7/): Open-source [forensics and intelligence gathering](https://null-byte.wonderhowto.com/collection/maltego/).
* [**Nmap**](https://nmap.org/): Port scanner and [network mapper](https://null-byte.wonderhowto.com/how-to/hack-like-pro-advanced-nmap-for-reconnaissance-0151619/).
* [**Wireshark**](https://www.wireshark.org/download.html): Graphical application for [network traffic analysis](https://null-byte.wonderhowto.com/news/8-wireshark-filters-every-wiretapper-uses-spy-web-conversations-and-surfing-habits-0134508/).

These tools can be installed using the below command.

apt-get install maltego metasploit-framework burpsuite wireshark aircrack-ng hydra nmap beef-xss nikto

Reading package lists... Done

Building dependency tree

Reading state information... Done

hydra is already the newest version (8.6-1kali1).

The following NEW packages will be installed:

beef-xss binfmt-support burpsuite fastjar fonts-droid-fallback fonts-lato

fonts-noto-mono ghostscript gsfonts imagemagick imagemagick-6-common

imagemagick-6.q16 jarwrapper java-wrappers javascript-common libc-ares2

libcupsfilters1 libcupsimage2 libdjvulibre-text libdjvulibre21 libdouble-conversion1

libfftw3-double3 libgmp-dev libgmpxx4ldbl libgs9 libgs9-common libhttp-parser2.8

libijs-0.35 libilmbase23 libjbig2dec0 libjs-jquery libjs-jquery-easing

libjs-jquery-fancybox libjs-jquery-mousewheel libjs-jquery-ui libjs-source-map

libjs-uglify libjxr-tools libjxr0 liblqr-1-0 liblua5.2-0 libmagickcore-6.q16-6

libmagickcore-6.q16-6-extra libmagickwand-6.q16-6 libnetpbm10 libnl-route-3-200

libopenexr23 libpaper-utils libpaper1 libpcre2-16-0 libqt5core5a libqt5dbus5

libqt5gui5 libqt5multimedia5 libqt5multimedia5-plugins libqt5multimediagsttools5

libqt5multimediawidgets5 libqt5network5 libqt5opengl5 libqt5printsupport5 libqt5svg5

libqt5widgets5 libruby2.5 libsbc1 libsmi2ldbl libspandsp2 libssh-gcrypt-4 libuv1

libwhisker2-perl libwireshark-data libwireshark11 libwiretap8 libwmf0.2-7

libwscodecs2 libwsutil9 libxcb-icccm4 libxcb-image0 libxcb-keysyms1 libxcb-randr0

libxcb-render-util0 libxcb-xinerama0 libxcb-xkb1 libxkbcommon-x11-0 libyaml-0-2

maltego netpbm nikto nodejs nodejs-doc openjdk-8-jre openjdk-8-jre-headless

qt5-gtk-platformtheme qttranslations5-l10n rake ruby ruby-addressable ruby-ansi

ruby-atomic ruby-buftok ruby-celluloid ruby-celluloid-io ruby-daemons

ruby-dataobjects ruby-dataobjects-mysql ruby-dataobjects-postgres

ruby-dataobjects-sqlite3 ruby-dev ruby-did-you-mean ruby-diff-lcs ruby-dm-core

ruby-dm-do-adapter ruby-dm-migrations ruby-dm-serializer ruby-dm-sqlite-adapter

ruby-docile ruby-domain-name ruby-em-websocket ruby-equalizer ruby-erubis

ruby-eventmachine ruby-execjs ruby-faraday ruby-geoip ruby-hitimes ruby-http

ruby-http-cookie ruby-http-form-data ruby-http-parser.rb ruby-json ruby-librex

ruby-libv8 ruby-memoizable ruby-mime-types ruby-mime-types-data ruby-minitest

ruby-mojo-magick ruby-msfrpc-client ruby-msgpack ruby-multi-json ruby-multipart-post

ruby-naught ruby-net-telnet ruby-nio4r ruby-oj ruby-parseconfig ruby-power-assert

ruby-public-suffix ruby-qr4r ruby-rack ruby-rack-protection ruby-ref ruby-rqrcode

ruby-rspec-expectations ruby-rspec-support ruby-rubydns ruby-simple-oauth

ruby-simplecov ruby-simplecov-html ruby-sinatra ruby-sqlite3 ruby-term-ansicolor

ruby-test-unit ruby-therubyracer ruby-thread-safe ruby-tilt ruby-timers ruby-tins

ruby-twitter ruby-uglifier ruby-unf ruby-unf-ext ruby-xmlrpc ruby-zip ruby2.5

ruby2.5-dev ruby2.5-doc rubygems-integration thin wireshark wireshark-common

wireshark-qt zip

The following packages will be upgraded:

aircrack-ng libcups2 libnl-3-200 libnl-genl-3-200 libxkbcommon0 metasploit-framework

nmap nmap-common

8 upgraded, 182 newly installed, 0 to remove and 458 not upgraded.

Need to get 381 MB of archives.

After this operation, 616 MB of additional disk space will be used.

Do you want to continue? [Y/n] y

**6Install the Latest Version of Tor**

[Tor](https://null-byte.wonderhowto.com/how-to/tor/) is available in Kali's repositories, but anonymity software should be acquired directly from the source (torproject.org). Furthermore, Kali's version of Tor is not reliably maintained or updated. This means we could be missing critical stability and security updates.

Add the Tor Project repositories to your APT repository list.

echo 'deb https://deb.torproject.org/torproject.org stretch main

deb-src https://deb.torproject.org/torproject.org stretch main' > /etc/apt/sources.list.d/tor.list

Then, download the Tor Project package signing key and import it into your APT keyring.

wget -O- 'https://pgp.mit.edu/pks/lookup?op=get&search=0xA3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD89' | sudo apt-key add -

-- https://pgp.mit.edu/pks/lookup?op=get&search=0xA3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD89

Resolving pgp.mit.edu (pgp.mit.edu)... 18.9.60.141

Connecting to pgp.mit.edu (pgp.mit.edu)|18.9.60.141|:443... connected.

HTTP request sent, awaiting response... 200 OK

Length: 47255 (46K) [text/html]

Saving to: ‘STDOUT’

- 100%[==================================================>] 46.15K 72.0KB/s in 0.6s

-- (72.0 KB/s) - written to stdout [47255/47255]

OK

You'll see the "OK" output when the signing key has been added to your keyring. Next, update APT using the below apt-get command.

apt-get update

Hit:1 http://downloads.metasploit.com/data/releases/metasploit-framework/apt lucid InRelease

Get:2 https://deb.torproject.org/torproject.org stretch InRelease [4,965 B]

Get:4 https://deb.torproject.org/torproject.org stretch/main Sources [1,169 B]

Get:5 https://deb.torproject.org/torproject.org stretch/main amd64 Packages [2,400 B]

Hit:3 http://archive-3.kali.org/kali kali-rolling InRelease

Fetched 8,534 B in 8s (1,091 B/s)

Reading package lists... Done

Install Tor using the below command, and you're done.

apt-get install tor deb.torproject.org-keyring

Reading package lists... Done

Building dependency tree

Reading state information... Done

Suggested packages:

mixmaster torbrowser-launcher socat tor-arm apparmor-utils obfs4proxy

The following NEW packages will be installed:

deb.torproject.org-keyring

The following packages will be upgraded:

tor

**7Configure File Sharing with Syncthing**

[Syncthing](https://github.com/syncthing/syncthing), created by [Jakob Borg](https://twitter.com/jakobborg), is a [cross-platform](https://github.com/syncthing/syncthing/releases/), private, lightweight file-syncing (Dropbox) alternative. As a penetration tester, transferring keystroke logs, screenshots, webcam recordings, and [sensitive loot files](https://null-byte.wonderhowto.com/how-to/hacking-windows-10-capture-exfiltrate-screenshots-remotely-0183646/#jump-step4) between [virtual private servers](https://null-byte.wonderhowto.com/how-to/white-hats-guide-choosing-virtual-private-server-0183135/) and local Kali machines can be a frustrating task. Syncthing makes secure file-sharing totally painless.

I've covered the [Syncthing installation and configuration](https://null-byte.wonderhowto.com/how-to/securely-sync-files-between-two-machines-using-syncthing-0185999/) in a previous article. Readers should reference that for a detailed step-by-step guide.

* **More Info:** [**How to Securely Sync Files Between Two Machines Using Syncthing**](https://null-byte.wonderhowto.com/how-to/securely-sync-files-between-two-machines-using-syncthing-0185999/)

**8Install a Code Editor**

[Atom](https://atom.io/) is a free, open-source, feature-rich, and highly customizable text editor. Its features include the ability to collaboratively share code in real time, intuitive coding autocompletion, and the ability to [install packages](https://atom.io/packages) which further enhance Atom's versatility. Other noteworthy text editors include [Geany](https://wiki.geany.org/) and [Gedit](https://wiki.gnome.org/Apps/Gedit).

To install Atom, head over to their website and download the latest [Debian installer](https://atom.io/download/deb). Next, open a terminal and install the required dependencies using the below apt-get command.

apt-get install gvfs gvfs-common gvfs-daemons gvfs-libs gconf-service gconf2 gconf2-common gvfs-bin psmisc

Reading package lists... Done

Building dependency tree

Reading state information... Done

Correcting dependencies... Done

The following NEW packages will be installed:

gconf-service (3.2.6-4.1)

gconf2 (3.2.6-4.1)

gconf2-common (3.2.6-4.1)

gvfs-bin (1.36.2-1)

libgconf-2-4 (3.2.6-4.1)

psmisc (23.1-1+b1)

The following packages will be upgraded:

gvfs (1.36.1-1 => 1.36.2-1)

gvfs-common (1.36.1-1 => 1.36.2-1)

gvfs-daemons (1.36.1-1 => 1.36.2-1)

gvfs-libs (1.36.1-1 => 1.36.2-1)

4 upgraded, 6 newly installed, 0 to remove and 462 not upgraded.

1 not fully installed or removed.

Need to get 3,317 kB of archives.

After this operation, 8,909 kB of additional disk space will be used.

Do you want to continue? [Y/n] y

Finally, use **dpkg**, a command line package manager, with the install (**-i**) argument.

dpkg -i ~/Downloads/atom-amd64.deb

(Reading database ... 191882 files and directories currently installed.)

Preparing to unpack atom-amd64.deb ...

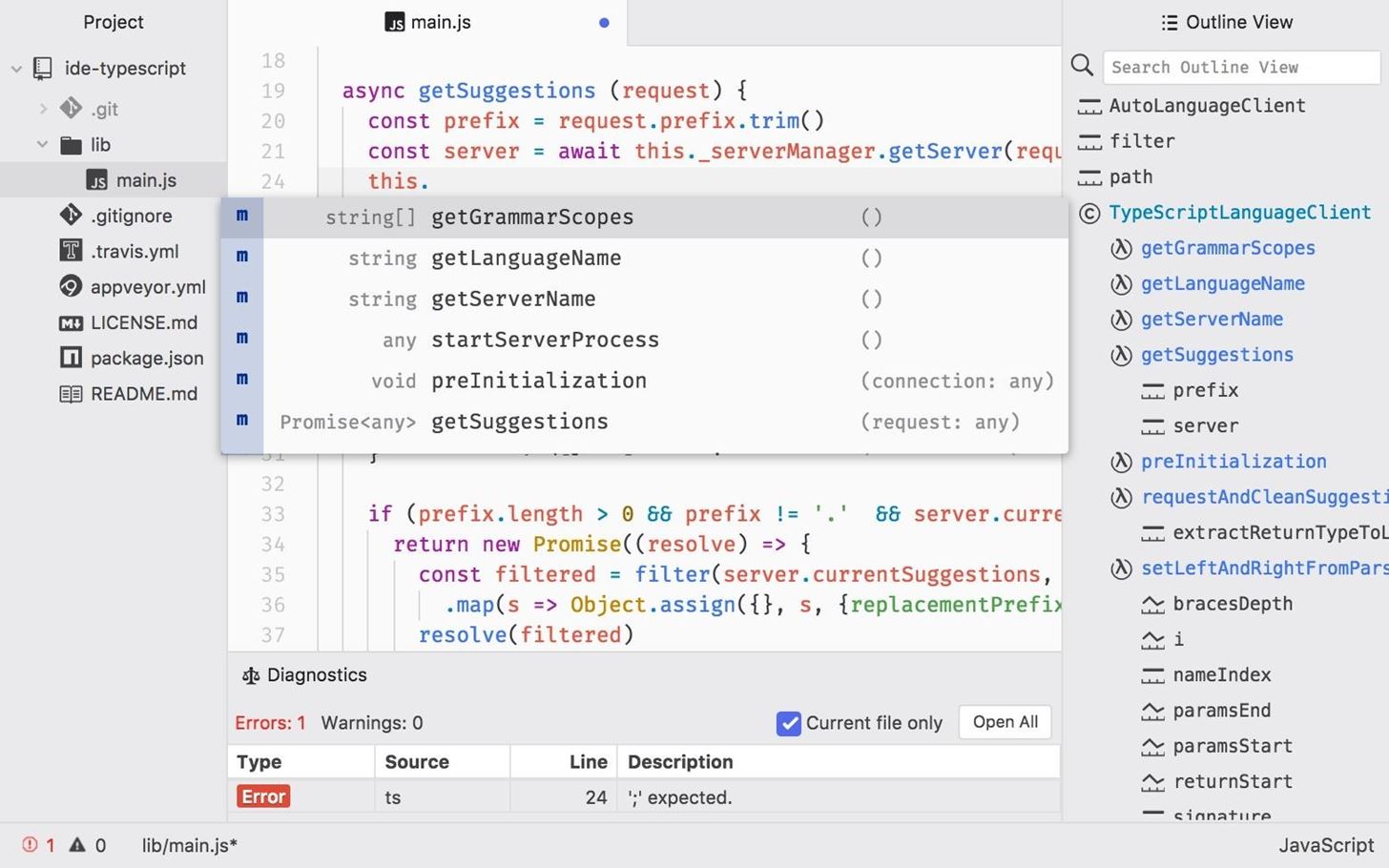
Unpacking atom (1.29.0) over (1.29.0) ...

Setting up atom (1.29.0) ...

Processing triggers for desktop-file-utils (0.23-3) ...

Processing triggers for mime-support (3.60) ...

When that's done, Atom will be available in your Applications menu.

[](https://img.wonderhowto.com/img/original/05/68/63669459068404/0/636694590684040568.jpg)

*Image via* [*Atom*](https://atom.io/)

**9Clone Rubber Ducky Encoder**

The [USB Rubber Ducky](https://null-byte.wonderhowto.com/collection/usb-rubber-ducky/) is the notorious keystroke injection tool. Creating [ducky payloads](https://null-byte.wonderhowto.com/how-to/use-usb-rubber-ducky-disable-antivirus-software-install-ransomware-0180418/#jump-step2) is easy using the [DuckToolKit website](https://ducktoolkit.com/), but as a penetration tester, it's unsafe to share client information with random websites. Uploading payload contents to a third-party website can be dangerous.

Instead, we can use **Git** to clone the USB Rubber Ducky [repository](https://github.com/hak5darren/USB-Rubber-Ducky) and encode payloads locally.

git clone https://github.com/hak5darren/USB-Rubber-Ducky

Cloning into 'USB-Rubber-Ducky'...

remote: Counting objects: 1657, done.

remote: Total 1657 (delta 0), reused 0 (delta 0), pack-reused 1657

Receiving objects: 100% (1657/1657), 31.88 MiB | 162.00 KiB/s, done.

Resolving deltas: 100% (745/745), done.

Checking out files: 100% (1509/1509), done.

Then, change ([**cd**](https://null-byte.wonderhowto.com/how-to/hack-like-pro-linux-basics-for-aspiring-hacker-part-2-creating-directories-files-0147234/)) into the USB-Rubber-Ducky/Encoder/ directory and use the following **java** command to start [encoding ducky payloads](https://www.hak5.org/gear/duck/writing-your-first-usb-rubber-ducky-payload) without third-party websites.

cd USB-Rubber-Ducky/Encoder/

java -jar encoder.jar -i input\_payload.txt -o inject.bin

**What's the First Thing You Do After Installing Kali?**

We all have varying degrees of interests, skill sets, and levels of experience. Which makes compiling a well-rounded list of post-installation steps tricky. Did I miss any critical steps? How do you personalize and customize new Kali install