GO H*CK YOURSELF

A simple introduction to cyber attacks and defense

BRYSON PAYNE

no starch press

GO H*CK YOURSELF

A Simple Introduction to Cyber Attacks and Defense

by Bryson Payne

no starch
press

San Francisco

First printing

25 24 23 22 21   1 2 3 4 5 6 7 8 9

ISBN-13: 978-1-7185-0200-0 (print)
ISBN-13: 978-1-7185-0201-7 (ebook)

Publisher: William Pollock
Managing Editor: Jill Franklin
Production Manager: Rachel Monaghan
Production Editor: Paula Williamson
Developmental Editor: Nathan Heidelberger
Cover Design: Monica Kamsvaag
Interior Design: Octopod Studios
Technical Reviewer: Bryan Fagan
Copyeditor: Paula Fleming
Compositor: Maureen Forys, Happenstance Type-O-Rama
Proofreader: Scout Festa
Indexer: JoAnne Burek

For information on book distributors or translations, please contact No Starch Press, Inc. directly:
No Starch Press, Inc.
245 8th Street, San Francisco, CA 94103
phone: 1.415.863.9900; info@nostarch.com
www.nostarch.com

Library of Congress Cataloging-in-Publication Data

```
Names: Payne, Bryson, author.
Title: Go h*ck yourself : a simple introduction to cyber attacks and defense
   / Bryson Payne.
Other titles: Go hack yourself
Description: San Francisco : No Starch Press, [2021] | Includes index.
Identifiers: LCCN 2021030107 (print) | LCCN 2021030108 (ebook) | ISBN
   9781718502000 (print) | ISBN 9781718502017 (ebook)
Subjects: LCSH: Penetration testing (Computer security)
Classification: LCC QA76.9.A25 P394 2021  (print) | LCC QA76.9.A25  (ebook)
   | DDC 005.8—dc23
LC record available at https://lccn.loc.gov/2021030107
LC ebook record available at https://lccn.loc.gov/2021030108
```

The information in this book is distributed on an "As Is" basis, without warranty. While every precaution has been taken in the preparation of this work, neither the author nor No Starch Press, Inc. shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in it.

About the Author

Dr. Bryson Payne is an award-winning cyber coach, author, and TEDx speaker, and the founding director of the Center for Cyber Operations Education at the University of North Georgia, an NSA-DHS Center for Academic Excellence in Cyber Defense. He is a tenured professor of computer science at UNG, where he has taught aspiring coders and cyber professionals since 1998, including coaching UNG's #1-in-the-nation NSA Codebreaker Challenge cyber operations team. In 2017, he received the University System of Georgia Chancellor's Service Excellence Leader of the Year Award. He has also been awarded the Department of the Army Commander's Award for Public Service medal from US Army Cadet Command and the Order of Thor medal from the Military Cyber Professionals Association. Dr. Payne was also recognized by the UNG Alumni Association as the 2021 Distinguished Professor.

Dr. Payne is a Certified Information Systems Security Professional (CISSP) and Certified Ethical Hacker (CEH), and he holds the elite SANS|GIAC GPEN, GRID, and GREM certifications. He has written over $45 million in successful grants for workforce development, technology education, and cybersecurity, and he has trained over 60,000 students through his online courses on coding and ethical hacking, including three top-rated Udemy courses. He was also the first department head of computer science at UNG and enjoys working with K–12 schools worldwide to promote computer science and cybersecurity education.

Dr. Payne holds a PhD in computer science from Georgia State University. Featured in the *Wall Street Journal*, *Campus Technology*, and *CIO* magazine, he is also the author of *Teach Your Kids to Code* and *Learn Java the Easy Way*, both published by No Starch Press. He has been programming, hacking, and reverse-engineering software for over 36 years; he sold his first paid program to *RUN Magazine* (Commodore 64) for its "Magic" column in 1985, for $10. In addition to his love for technology, Dr. Payne enjoys learning languages and speaks Spanish, French, Russian, and Mandarin Chinese.

About the Technical Reviewer

Bryan Fagan is a coding enthusiast living in Dahlonega, Georgia, where he spends most of his time teaching high school students about cybersecurity. He has started several afterschool programs focused on engineering, technology, and digital game design.

2

PHYSICAL ACCESS HACKS

Have you ever left your laptop unattended in a coffee shop, thinking that your private files would be safely protected behind a login screen? It turns out that anyone with physical access to your computer can gain access to your files with just a few keystrokes, without needing to know your login details. In this chapter, I'll show you two *physical access hacks*: the *Sticky Keys hack*, used on Windows PCs, and the *Mac root hack*, used on Macs. Both hacks give an attacker administrator-level access to the target computer, allowing them to steal files or change important settings.

Physical access hacks may sound scary because they can be used maliciously by attackers on stolen or unattended computers. However, they also have constructive applications. Ethical hackers at home and at IT help desks use techniques like the Sticky Keys hack or the Mac root hack to recover files that would otherwise be lost due to a forgotten password. If you have an old computer in the garage or attic with family photos or other important documents that you can't access because no one remembers the computer's password, these hacks can help.

WARNING Do not *perform either of these hacks on your main computer, because they could leave your machine vulnerable to attack. You can usually find an old desktop or laptop if you ask around. Get creative, but stay ethical; be sure to get the owner's permission before trying out these hacks on someone else's computer. If you can't find an extra Windows or Mac computer to practice on, you can still read this chapter to understand the dangers of physical access attacks.*

The Sticky Keys Hack

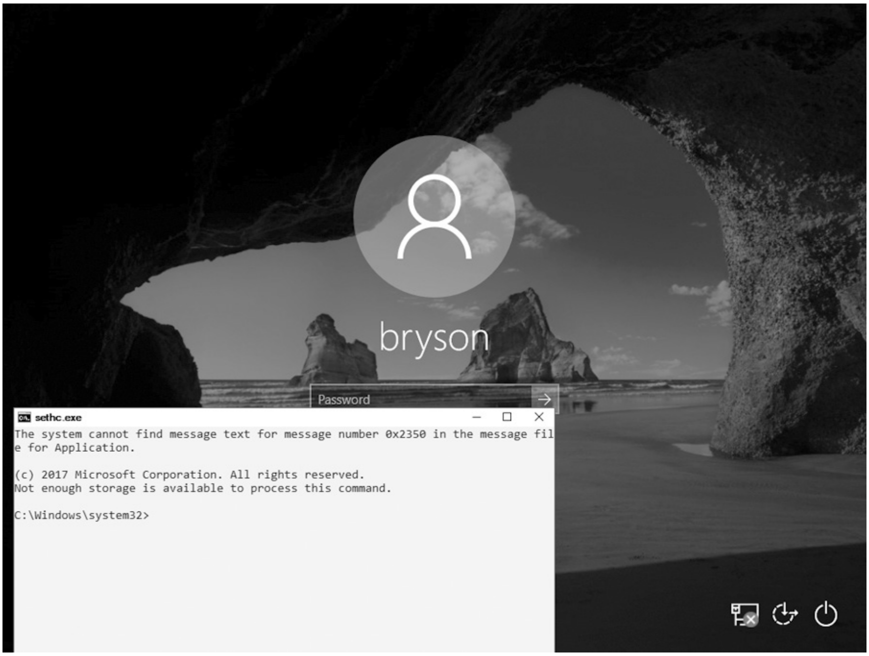
Sticky Keys is a Windows feature that makes it easier to issue certain keyboard commands, like CTRL-C to copy or CTRL-V to paste, by allowing you to press the keys one after another instead of all at once. Sticky Keys is triggered by pressing SHIFT five times and can even be turned on from the Windows login screen, before a username or password has been entered.

For this hack, we'll replace the Sticky Keys program file with another file, *cmd.exe*. That way, instead of launching the usual Sticky Keys assistant, pressing SHIFT five times will launch a *command prompt*. This is a text-based program that lets us enter commands directly into Windows. By launching a command prompt at the login screen (see Figure 2-1), you'll be able to add a new username and password, give yourself administrator-level access to the computer, and access the computer's files, all without knowing the login information on that computer!

Since Windows 10 computers that have been updated in 2019 or later are safe from the Sticky Keys hack, you'll need an older Windows computer to try out the hack for yourself. You'll also need a Windows 10 installation disc or USB drive. To create one, follow the instructions in Appendix A.

Booting from a Windows 10 Installation Disc

To replace the Sticky Keys program with the command prompt program, we need to access the hard drive that contains those program files using a Windows 10 installation disc or USB drive. Once you've created an installation disc, as described in Appendix A, insert the disc and then restart the computer.



```
The system cannot find message text for message number 0x2350 in the message fil
e for Application.

(c) 2017 Microsoft Corporation. All rights reserved.
Not enough storage is available to process this command.

C:\Windows\system32>
```

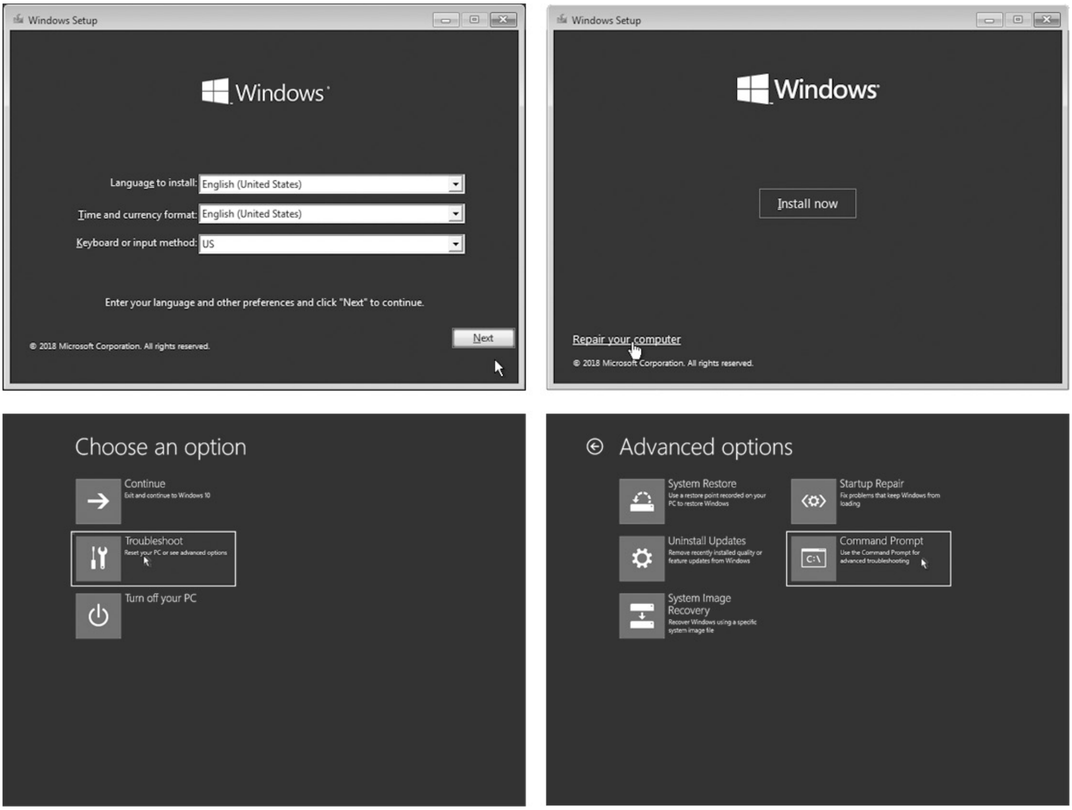
Figure 2-1: The Sticky Keys hack brings up a command prompt window instead of the Sticky Keys assistant.

We need to tell the computer to load the operating system (OS) from the disc or USB drive instead of from the computer's hard drive. To do this, we'll access either the boot menu or the *Basic Input/Output System (BIOS)*, which contains basic settings that control your computer when it starts up. Different PC manufacturers and different versions of Windows cause the instructions to vary a bit, but the following steps combined with a little web searching will get you into most older Windows computers:

1. On Windows computers, you press a special key to access the boot menu or BIOS. If your startup screen doesn't show you which key to press just before the Windows startup logo appears, reboot your computer and quickly press ESC, DELETE, F8, F9, F10, F11, or F12 right as it begins to start up. Search online for "boot menu" and the specific make and model of your computer to find the right key.
2. If the boot menu appears, select the **Boot from DVD** or **Boot from USB** option to boot from the Windows installation disc you inserted, then move on to step 5.
3. If the boot menu doesn't appear after a few restarts, try entering the BIOS menu instead: turn the computer off and on again, and press DELETE, F2, F9, F10, F12, or ESC. Search online for "BIOS" and your computer model to find the right key.

4. Once you're inside the BIOS, find the boot options and change the order or priority of your boot devices (often by using your arrow keys) to make the USB or DVD the top option. Then save the changes and exit the BIOS.
5. Reboot the computer again. You should briefly see the message `Press any key to boot from CD or DVD` or `Press any key to boot from USB device`. Press any key (such as the spacebar) *immediately* to boot from your DVD or USB.
6. When the Windows installation disc starts up, click **Next ▸ Repair your computer ▸ Troubleshoot ▸ Command Prompt**, as shown in Figure 2-2. The menu order or the option names might look different, but look for the Windows command prompt.

WARNING *Make sure you* don't install *Windows 10—that would wipe out all the files from the PC you're trying to recover!*


Windows Setup
Windows
Next
Windows Setup
Windows
Install now
Repair your computer
Choose an option
Continue
Exit and continue to Windows 10
Troubleshoot
Reset your PC or see advanced options
Turn off your PC
Advanced options
System Restore
Use a restore point recorded on your PC to restore Windows
Startup Repair
Fix problems that keep Windows from loading
Uninstall Updates
Remove recently installed quality or feature updates from Windows
Command Prompt
Use the Command Prompt for advanced troubleshooting
System Image Recovery
Recover Windows using a specific system image file

Language to install: English (United States)

Time and currency format: English (United States)

Keyboard or input method: US

Enter your language and other preferences and click "Next" to continue.

© 2018 Microsoft Corporation. All rights reserved.

© 2018 Microsoft Corporation. All rights reserved.

Figure 2-2: Use the Windows installation disc to access the command prompt.

7. Once you've reached the Windows command prompt (usually a black, text-based window), type **c:** and press **ENTER** to change to the C: drive, as shown here:

```
X:\> c:
```

8. Enter the command **dir** to see a list of files and folders on the C: drive. Look for a folder called *Windows* (it will be marked `<DIR>`, short for *directory*).

```
C:\> dir
 Volume in drive C is Windows 10
 Volume Serial Number is B4EF-FAC7
 Directory of C:\
--snip--
03/15/2018  02:51 AM    <DIR>           Users
05/19/2019  10:09 AM    <DIR>           Windows ❶
--snip--
```

   This folder ❶ contains the operating system files, including the command prompt application and the Sticky Keys program file that we need to swap out to perform this hack.

9. If there's no *Windows* directory on the C: drive, try the same process in the D: drive by entering **d:** and then **dir**. If the D: drive doesn't have the *Windows* directory either, keep going through the alphabet (E:, F:, G:, and so on) until you find a drive containing *Windows* in its listing.

Gaining Administrator-Level Access

Now to replace the *sethc.exe* Sticky Keys program with the *cmd.exe* command prompt program. Then we'll be able to create a new administrator account on the computer.

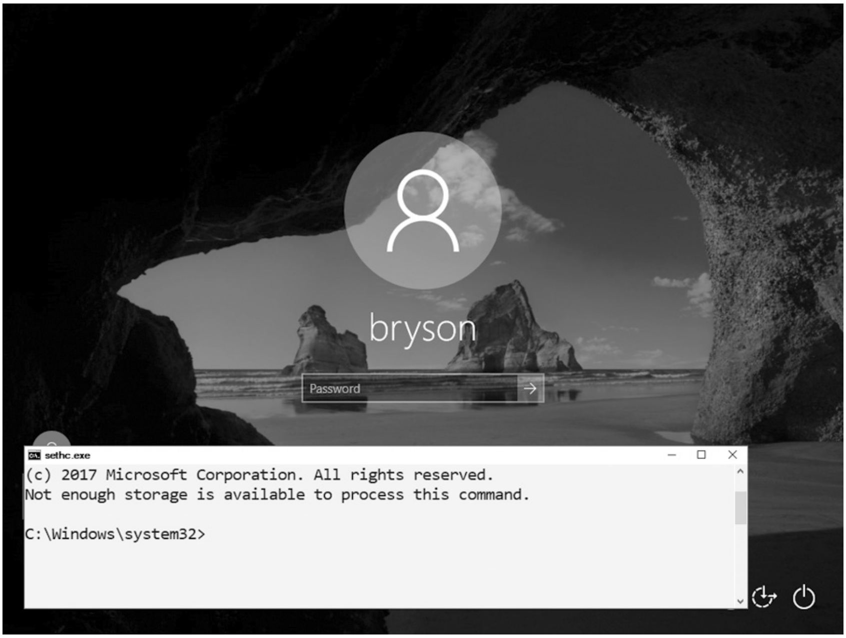
1. Enter the following three commands:

```
C:\> cd \Windows\System32\
C:\Windows\System32\> copy sethc.exe sethc.bak
C:\Windows\System32\> copy cmd.exe sethc.exe
```

   These commands enter the directory where we can find both *sethc.exe* and *cmd.exe*, create a backup copy of the Sticky Keys program, and replace the original Sticky Keys program file with a copy of the command prompt program file. This way, whenever the computer runs *sethc.exe*, it will open a command prompt window in place of the Sticky Keys program.

2. After the third command, Windows will ask you if you want to overwrite *sethc.exe*. Enter **Y** to proceed.

3. Remove the Windows 10 installation DVD or USB and reboot the computer.
4. When the PC boots to the login screen, press **SHIFT** five times. Instead of the usual Sticky Keys program, you should see a command prompt window pop up *in front* of the login screen, as shown in Figure 2-3.



```
(c) 2017 Microsoft Corporation. All rights reserved.
Not enough storage is available to process this command.

C:\Windows\system32>
```

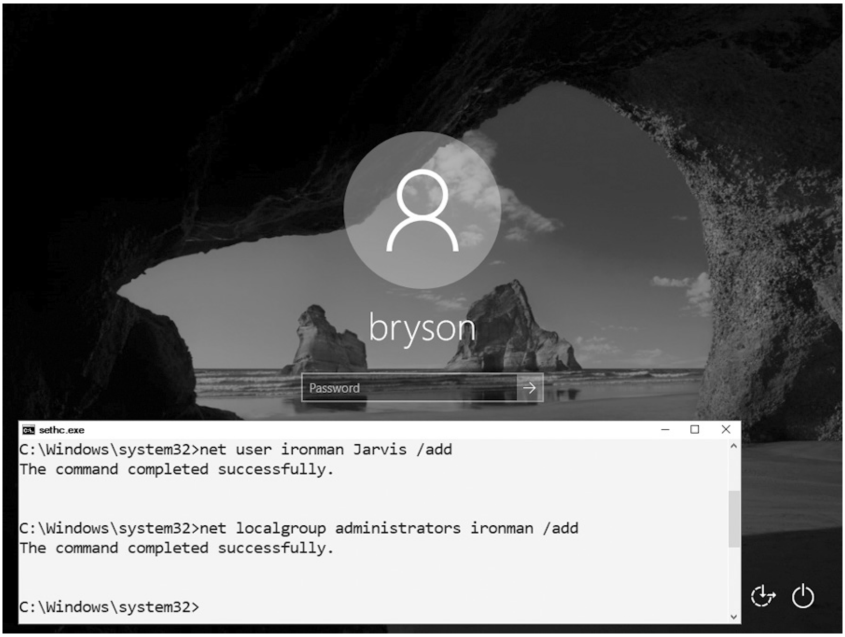
Figure 2-3: Opening a command prompt window

5. Enter the following two commands into the command prompt window:

```
C:\Windows\System32\> net user ironman Jarvis /add
C:\Windows\System32\> net localgroup administrators ironman /add
```

The first command adds a user account named *ironman* with the password *Jarvis* to the Windows computer. The second command adds the *ironman* user to the list of local administrators. This means that when we log in as *ironman*, we'll have administrator-level access to all the files on the computer.

6. When you see a success message like the one in Figure 2-4, close the command prompt.



```
C:\Windows\system32>net user ironman Jarvis /add
The command completed successfully.


C:\Windows\system32>net localgroup administrators ironman /add
The command completed successfully.


C:\Windows\system32>
```

Figure 2-4: We've successfully added a user named ironman *as an administrator on this computer.*

In addition to creating a new user account, you can also reset the password of an existing user from the command prompt window by entering **`net user`** followed by the existing username and the new password you want to set—for example, `net user bryson Thisisyournewpassword!`. However, you should never reset another person's password without their permission and the permission of the computer's owner.

Now You're an Administrator. Log In!

Congratulations! You now have access to the machine as an administrator. Go ahead and log in. Enter **`.\ironman`** as the username (or select **ironman** from the list of accounts, as shown in Figure 2-5). The dot and backslash before `ironman` tell Windows the account is local to the computer and not stored on a network server. After entering the username, enter the password, **`Jarvis`**.

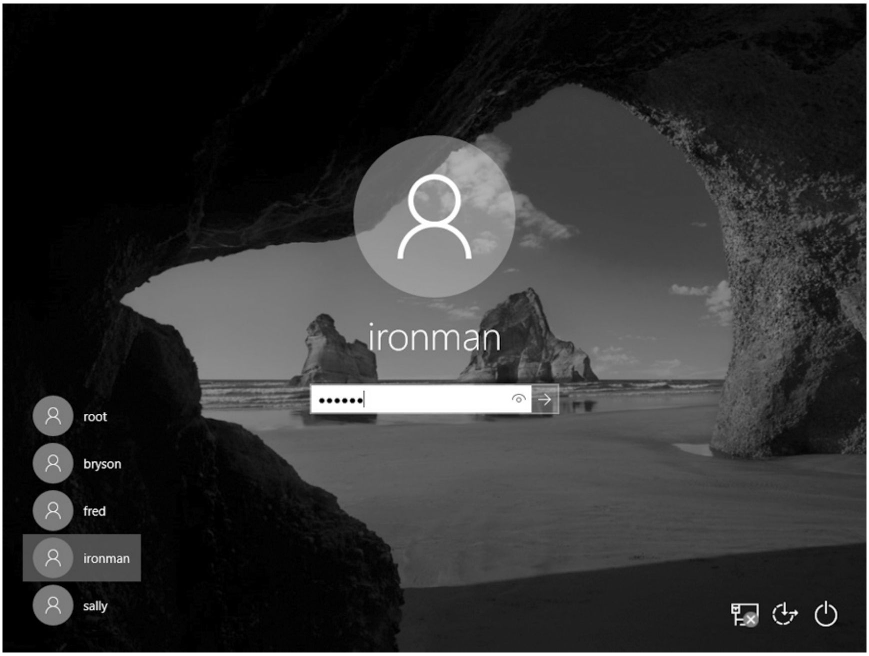
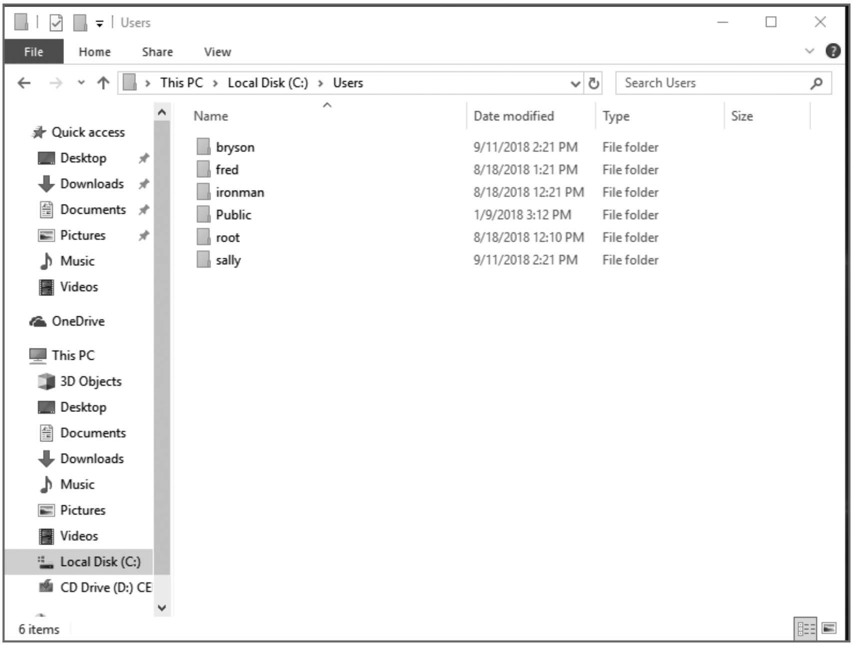


Figure 2-5: You can now use the ironman *user to log in to this Windows PC.*

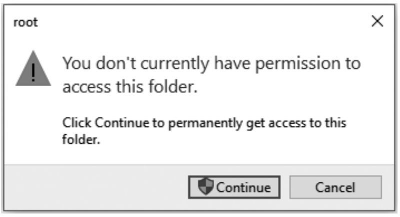
Since we made the *ironman* user a member of the local administrators group, you should have administrator-level access to *all* files and folders, including all users and documents in *C:\Users\*, as shown in Figure 2-6.



Name	Date modified	Type	Size
bryson	9/11/2018 2:21 PM	File folder	
fred	8/18/2018 1:21 PM	File folder	
ironman	8/18/2018 12:21 PM	File folder	
Public	1/9/2018 3:12 PM	File folder	
root	8/18/2018 12:10 PM	File folder	
sally	9/11/2018 2:21 PM	File folder	

Figure 2-6: As an administrator-level user, you can see all *users' files, not just your own.*

When you click into another user's folder for the first time, you'll see a pop-up message saying you need permission to open another user's files, as shown in Figure 2-7. Since you're an administrator, click **Continue** to grant yourself permanent access!



root

You don't currently have permission to access this folder.

Click Continue to permanently get access to this folder.

Figure 2-7: Administrators can give themselves permission to access anyone's files on the same computer.

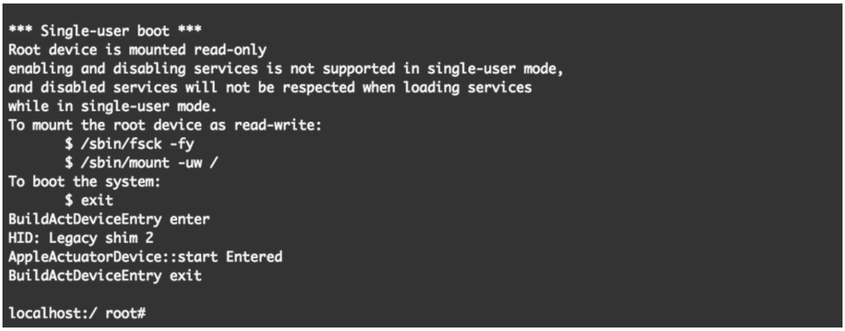
The Sticky Keys hack works only on Windows machines. However, computers running macOS are vulnerable to physical access hacks as well.

The Mac Root Hack

Like the Sticky Keys hack, the Mac root hack is a physical access attack that will give you administrator-level access to a computer. It makes you a *root* user, which is the administrator-level account on macOS computers. For this hack, all you need is a Mac computer. We'll reboot the Mac in *single-user mode*, a troubleshooting and repair login. From there, we can change the root user's password, giving us access to all the files on the computer.

Updating the Root User Settings

1. To begin, the Mac needs to be completely turned off—not just asleep. If it isn't off already, press and hold the power button for about six seconds.
2. Press the power button again while holding COMMAND-S (⌘-S) to enter single-user mode. You should see a text-based command line terminal window with very few features, as shown in Figure 2-8.



```
*** Single-user boot ***
Root device is mounted read-only
enabling and disabling services is not supported in single-user mode,
and disabled services will not be respected when loading services
while in single-user mode.
To mount the root device as read-write:
       $ /sbin/fsck -fy
       $ /sbin/mount -uw /
To boot the system:
       $ exit
BuildActDeviceEntry enter
HID: Legacy shim 2
AppleActuatorDevice::start Entered
BuildActDeviceEntry exit

localhost:/ root#
```

Figure 2-8: Part of the single-user mode boot screen on a Mac

The terminal prompt should contain `root#` (press ENTER a few times if it's not visible on the last line, and it should come up), indicating that we're logged in to the command line as the root, or administrator, user.

3. Enter the following commands to mount, or connect to, the hard drive:

```
localhost:/ root# /sbin/fsck -fy
localhost:/ root# /sbin/mount -uw /
```

4. Now connect to the Open Directory service's property list, or *plist*:

```
localhost:/ root# launchctl load /System/Library/LaunchDaemons/com.apple.opendirectoryd.plist
```

Your Mac uses Open Directory to track users, groups, file sharing, and even Wi-Fi printers. Think of it as a catalog of all the user accounts and permissions on your Mac.

5. If you get an error after running the previous command, try running the following command instead—it's the same as step 4, but for older Macs:

```
localhost:/ root# launchctl load /System/Library/LaunchDaemons/com.apple.DirectoryServices.plist
```

6. Now to change the root user's password. Enter this command:

```
localhost:/ root# passwd
```

7. Enter a new password. You won't see the characters of the password on the screen as you type. Then enter the password a second time to confirm the change. (If you mistype the password, start up in single-user mode again and do this same hack—it should reset the root user's password every time.)

NOTE *To change any other user's password while you're logged in as* root, *enter* **`passwd`** *followed by the username you want to change (such as* `passwd bryson`*). You might be prompted for the root user password you just set; if so, enter it. Then type the user's new password and press* ***ENTER****. Type the new password a second time and press* ***ENTER*** *again, and you'll be able to log in as that user using the password you set.*

You're the Root User Now!

Well done! Now that you've changed the root user's password to something you know, you can log in as the root user anytime you want. Try it out right now: either enter **`reboot`** at the command line to reboot the computer or press the power button to turn the computer off and back on. When the computer boots normally to the Mac login screen, enter **`root`** as the username and type in the new password you've just set, as shown in Figure 2-9.

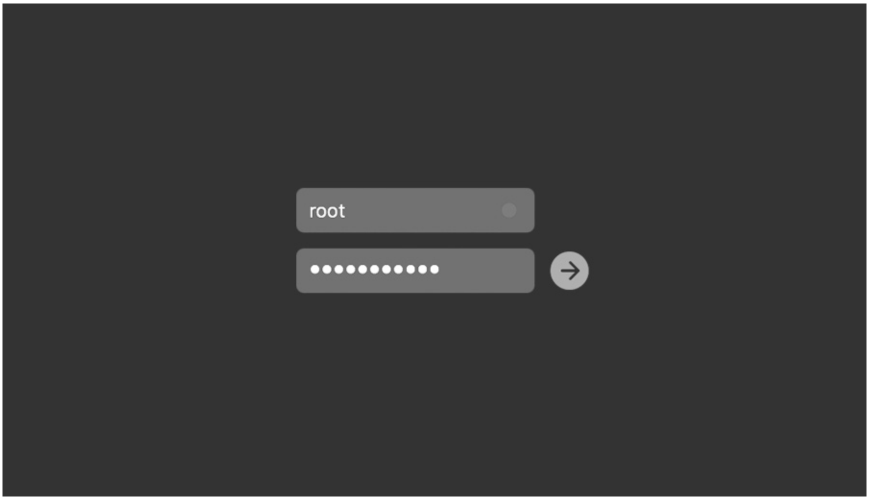


Figure 2-9: After the Mac root hack, you can log in as the root user with the password you set in the hack.

Click through any setup screens you see, and you'll soon come to the Mac desktop. You should see in the menu bar at the top of the screen that you're logged in as the system administrator. You now have access to all users' files and folders on the Mac!

Other Physical Hacks

There are many physical access hacks besides the Sticky Keys hack and the Mac root hack. In fact, almost any bootable disc—like Ultimate Boot CD, KNOPPIX, SystemRescueCd, or Trinity Rescue Kit—can give you access to the files on the hard drive of a computer you have physical access to. There are also specially made hacking tools, like Rubber Ducky and Bash Bunny, that cost under $100 and look like regular USB drives but contain automated tools for hacking into computers. Some physical access hacks even use voice commands. For example, the Open Sesame! attack used Microsoft's Cortana voice assistant to bypass the login screen by telling Cortana to open a malicious file on a USB drive or website.

Protecting Against Physical Hacks

As you've seen, physical access hacks can help you recover old photos, copy files, and change users on almost any computer you can physically touch, even without the original password. However, that means anyone who has physical access and knows these hacks can access *your* private files and information too! That's why it's important to keep your devices with you or locked away in a secure area.

If someone manages to get access to your computer, however, there are a few ways to protect your data. One is to set a *firmware password*, also called a *BIOS password* or *EFI password*. This option on Macs and most PCs can prevent attackers from tampering with your computer's BIOS/UEFI settings, neutralizing hacks like the Sticky Keys hack and Mac root hack. Unfortunately, firmware passwords are only one layer of defense and can often be bypassed. For example, motivated attackers can remove a battery from the circuit board in your computer, thereby erasing the stored firmware password on most PCs.

A surer bet is to *encrypt* your files, scrambling them into an unreadable form that can only be *unencrypted* (unscrambled) with a password. The encryption password is different from your computer's login password, so an attacker can't see what's inside your encrypted files by changing your user password with the Sticky Keys or Mac root hack. We'll discuss encryption in more detail in Chapter 11.

The Takeaway

In this chapter, you saw how to use the Windows Sticky Keys hack and Mac root hack to gain administrator-level access to all the files and user accounts on a computer, even when you don't know the username and password. You also learned that there are other physical hacks and some specialized tools, like Rubber Ducky and Bash Bunny, that make physical hacks even easier. While you can use these hacks to recover lost files or reset a forgotten password, you also discovered that an attacker with physical access to your computer can often gain access to every bit of your information. You can defend against these hacks by limiting who has access to your computer, setting a firmware password, and encrypting your files.

Now that you understand the importance of physical security, it's time to start thinking about other attacks that can put your computer in danger—malicious websites, phishing and infected email attachments, and even attacks on the internet-connected smart devices in your daily life. To be able to practice these other types of hacks safely, and to learn to defend against them, you'll set up your own private virtual hacking lab in Chapter 3.