HOW CYBERSECURITY REALLY WORKS

A HANDS-ON GUIDE FOR TOTAL BEGINNERS

SAM GRUBB

EARLY ACCESS

no starch press

NO STARCH PRESS EARLY ACCESS PROGRAM: FEEDBACK WELCOME!

Welcome to the Early Access edition of the as yet unpublished *How Cybersecurity Really Works* by Sam Grubb! As a prepublication title, this book may be incomplete and some chapters may not have been proofread.

Our goal is always to make the best books possible, and we look forward to hearing your thoughts. If you have any comments or questions, email us at **earlyaccess@nostarch.com**. If you have specific feedback for us, please include the page number, book title, and edition date in your note, and we'll be sure to review it. We appreciate your help and support!

We'll email you as new chapters become available. In the meantime, enjoy!

HOW CYBERSECURITY REALLY WORKS

SAM GRUBB

Early Access edition, 2/25/21

ISBN-13: 978-1-7185-0128-7 (print)
ISBN-13: 978-1-7185-0129-4 (ebook)

Publisher: William Pollock
Executive Editor: Barbara Yien
Production Editor: Rachel Monaghan
Project Editor: Dapinder Dosanjh
Developmental Editor: Frances Saux
Cover Illustrator: Gina Redman
Interior Design: Octopod Studios
Technical Reviewers: Cliff Janzen
Copyeditor: Anne Marie Walker
Compositor: Craig Woods, Happenstance Type-O-Rama
Proofreader: Rachel Head

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.

CONTENTS

The chapters in **red** are included in this Early Access PDF.

1

AN INTRODUCTION TO CYBERSECURITY

Cybersecurity is a vast and diverse field. Whether you're setting up a firewall or creating a password policy, your actions impact all levels of an organization, from its technicians and help desk to the CEO. Cybersecurity also affects every piece of technology in an organization: mobile phones, servers, and even devices like industrial control systems. A field this extensive and deep can be a little intimidating when you first enter it. This is especially true if you're trying to learn about cybersecurity without entering the field. For example, you might be an IT department head who wants to learn more so you can better protect your organization.

This chapter starts slow: we'll talk about what cybersecurity is and isn't, as well as the difference between white hat and black hat hackers.

What Is Cybersecurity?

At its core, cybersecurity has one driving purpose: to identify cyber threats in an organization, calculate the risk related to those threats, and handle those threats appropriately. Not every threat that a company experiences is an issue that cybersecurity deals with directly (for example, pandemics or physical damage to a building caused by a tornado or flood). In general, cybersecurity uses the *CIA triad* model to determine which threats are under its purview.

The CIA triad consists of three categories of security: confidentiality, integrity, and availability. *Confidentiality* involves how assets and data are exposed to people or processes, and ensures that only the people who are supposed to access a resource can access it. *Integrity* ensures that assets and data aren't changed without proper authorization. This not only includes items like entries in a database server, but also adding a user to a network, for example. *Availability* ensures that data or assets are accessible when needed. For work to continue, you must be able to access data when necessary.

Figure 1-1 shows the elements of the CIA triad positioned in a triangle to demonstrate how you might need to balance each of them to maintain the functionality of the others. For example, if you focus too much on confidentiality, you risk significantly locking down your assets so no one else can use that data for their job, creating an availability issue. Similarly, by placing too much emphasis on integrity, you lose confidentiality, because you must be able to read data to ensure that nothing has changed. By balancing the three triad components, you can achieve equilibrium between the core elements that encompass what cybersecurity does on a regular basis.

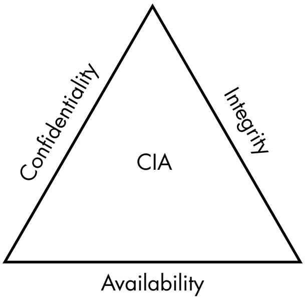


Figure 1-1: The CIA triad

Some experts debate the merits of adding elements to the traditional triad to contend with new technologies or priorities within cybersecurity. One element often added is *non-repudiation*, which is the idea that when a person or entity does something, there must be specific evidence tying them to that action so it's impossible for them to deny they did it.

Cybersecurity and Privacy

In recent years, there has been an emphasis on the relationship between cybersecurity and privacy. In this situation, privacy means the rights and abilities of a person to control how information about them is stored, shared, and used. Although the topic of privacy extends beyond cybersecurity, cybersecurity still plays a huge role in ensuring that an individual's data is secured against malicious use. Cybersecurity is also responsible for many of the controls that allow a company to audit its data use, ensuring that it follows any necessary rules or regulations. Going forward, the protection of a user's privacy will likely become an increasingly integral part of the cybersecurity field.

What Cybersecurity Isn't

In a field as large as cybersecurity, you're bound to encounter a few distorted ideas about its scope. To mitigate these misconceptions, it's best to discuss what cybersecurity isn't. Doing so will help define the field and what it actually means to *do* cybersecurity.

First, cybersecurity isn't synonymous with hacking. The media would have you believe that all cybersecurity professionals do is clack away at a keyboard, trying to break into a system. Although *penetration testing*—the act of attempting to break into a system you're authorized to attack, such as your own or a client's, to discover vulnerabilities from an attacker's perspective—is a part of cybersecurity, it's but one section of the field. A *vulnerability* is a flaw in a system, including how it's set up or how people use it. For example, having an error in a system's code can cause a vulnerability. Attackers create *exploits* to take advantage of vulnerabilities. But just because you don't know how to execute an exploit using a flaw in a computer's memory doesn't mean you can't be an expert in setting up and maintaining firewalls. This means that you don't need to understand how every hacking tool works or exactly what the latest exploit does to contribute to the cybersecurity industry.

Second, cybersecurity isn't switch flipping. Some people use the term *switch flipping* to describe what they think system engineers or other IT professionals do: they just flip switches or configure systems without understanding the underlying processes that make a system work. It's true that configuring a system to be secure is vitally important to cybersecurity. But securing a system can't necessarily be done by following a checklist. It requires looking at the entire system, noting how every component interacts not only with the other components, but also with other systems to fully understand how to secure a system. In addition, professionals need deliberation and critical thinking skills to know how to secure a system in situations where it's impossible to apply best practices.

Third, cybersecurity doesn't only require technical skills. Just as important as technical knowledge is the ability to translate that information into tips and resources that everyone can understand when professionals give presentations or write reports. Cybersecurity professionals work with every department in an organization, which means their interpersonal communication skills are essential. The only way your organization will become more secure is if everyone understands their role in maintaining security, which means you must communicate that role effectively.

Black Hats vs. White Hats

When you think of the term *hacker,* you probably think of someone doing something malicious to or with a computer, such as destroying files or unlocking electronic locks on doors so robbers can break in. The reason you think this way is that the media generally uses the word *hacker* to describe computer criminals. But not all hackers are hoodie-clad teenagers in basements banging on a keyboard while listening to death metal. In fact, people from all different backgrounds and regions participate in computer crime. The term *hacker* is also used to describe good cybersecurity experts: the label applies to anyone who asks questions and breaks systems, whether they're computers or physical devices, to learn more about them, not necessarily just to commit crimes. Many specific expressions, such as *bad actor, attacker,* and *state actor,* single out cybercriminals. But in this book, I'll call them *black hats* (as well as *attackers* or *adversaries*).

As just mentioned, attackers come from different backgrounds and places, but they all share the same intent: to use their technical knowledge to commit a crime. These crimes often revolve around financial gain of some sort, either directly by stealing money or demanding ransom payments, or indirectly by stealing important information, such as social security numbers to sell at a later time. It's important to note that not every adversary is pursuing money. They could be seeking specific information or trying to disrupt a service. There are many arguments about what constitutes a crime when it comes to malicious computer use. For the purposes of this book, I consider any violation of the current United States Computer Fraud and Abuse Act to fit the definition of cybercrime.

On the other side of the spectrum are the white hats. *White hats* are cybersecurity experts who apply their technical knowledge to making systems more secure. They not only include people who work for a company's security department, but also independent professionals who conduct security research, such as analyzing malware or discovering *zero-day* vulnerabilities (brand-new, never-before-seen vulnerabilities in a system or software). These people work tirelessly to try to stay one step ahead of black hats.

In a gray area in the middle are *gray hats.* The activities of a gray hat aren't necessarily malicious, but they're not honorable either. For example, attacking a system without permission to find vulnerabilities that you then disclose to the system's owner is a gray area, because typically white hats don't perform any attacks without permission. Which side a gray hat falls on depends on a person's perspective. If someone uses their skills to get past a government filter on the internet, they might look like an attacker to the government but a white hat to everyone trying to exercise freedom of speech.

Types of Black Hats

Although a wide variety of people fit the role of a black hat, you can still group them into categories. These categories are not meant to be exhaustive but should give you a general idea of the motivations behind black hat activity.

Script Kiddies

Script kiddies are adversaries who have no inherent skill and follow instructions found on the internet to execute their attacks. They generally find prewritten scripts (hence the name *script kiddie*) built to run a specific type of attack. They then enter their target information and fire off the script. Traditionally, script kiddies pose a low threat to most organizations. The attacks they use aren't usually sophisticated and often rely on outdated or easily recognized vectors of attack. But script kiddies shouldn't be taken lightly. Just because they don't have the skills of more elite black hats doesn't mean they can't do damage given the right set of tools.

Organized Criminals

A growing sector of organized crime is turning to black hat activities as government policing cuts off their other sources of revenue. Organized crime is highly effective at recruiting people with expert skills. As a result, these attackers use the latest vulnerabilities, create their own malware, and do extensive research to obtain large financial payoffs for their work. This makes them significant threats. Eastern Europe and Russia are particular hotbeds for this type of activity.

Hacktivists

A *hacktivist* is a person or group who uses hacking skills for a political purpose. They usually try to deface or disrupt services rather than stealing data or money. For example, a hacktivist group might take possession of the Twitter account of a company they disagree with, using the account to write terrible messages to smear the company's reputation or promote their own agenda. One of the most legendary hacktivist groups is Anonymous, which generally targets governments or other organizations it believes are authoritative in nature. It has taken down websites and released leaked documents, among a number of other activities (although it's hard to know exactly what the group has accomplished, because anyone can claim to be a member). Hacktivists can pose a significant threat to organizations and are generally more skilled than script kiddies.

State Actor

A *state actor* is a black hat who works for a government. To many, these agents operate in the gray area, because the legitimacy of their actions might seem to vary depending on which government they happen to work for. Nevertheless, state actors use the same techniques as other attackers, and their attacks can cause significant damage. State actors are typically interested in either stealing proprietary information to help their nation or disrupting services to hurt a foreign nation. China, North Korea, Iran, and Russia have robust programs connected to several major black hat campaigns, including breaches into Sony to steal sensitive internal documents and disruptions to elections worldwide. State actors pose some of the highest risks because they're well funded and they operate with the latest technology and training.

Advanced Persistent Threats

A more recent term, an *Advanced Persistent Threat (APT)* describes an attack that remains hidden for an extended period, slowly digging deeper into its target system until it meets its goals. Originally, state actors were the only types of adversaries with the resources and expertise to perform this type of attack. But in recent years several non-government groups have been able to execute similar operations. APTs are extremely dangerous, because it's difficult to identify where they are in your organization, what they might have access to, or who they've compromised. APTs run the gamut of motivation from targeted data theft to straight ransom.

Types of White Hats

Just like black hats, white hats fill a diverse variety of roles needed for a successful cybersecurity program. Cybersecurity isn't a monolith; it covers a multitude of fields and areas of expertise, and it's extremely difficult for one person to handle it alone. Organizations that cannot afford a dedicated security team should consider seeking outside help to supplement their own internal IT staff and provide advice where required.

The following sections explain various white hat positions along with a brief description of the typical tasks of each position. This list is by no means exhaustive, nor should it be considered standard, because some organizations might have different needs or differing ideas about where a position fits in their internal structure. That said, this list should provide you with a good idea of the types of positions that exist and the skills a person needs to fill specific roles. Also, note that I don't mention any educational degrees. The reason is that most roles in cybersecurity don't require any specific degree; instead, they rely heavily on knowledge and experience (both of which can be accumulated elsewhere). I've encountered experts with advanced cybersecurity degrees and others who had master's degrees in military history. Even so, it might take longer to gather the necessary knowledge and experience without a degree.

Cybersecurity/Security Operations Center Analysts

A *cybersecurity analyst* is an entry-level role tasked with maintaining and monitoring alerts that come in from various cybersecurity tools or devices. Their primary job is to find anything that looks suspicious and send it up the chain for further analysis if necessary. Often, these roles are tied into a *Security Operations Center (SOC)*, a facility where systems aggregate and monitor alerts from across an organization.

Analysts are the first responders for many security incidents, because they're the ones getting the alerts or directly contacting end users. These jobs typically require a strong IT background: additional security experience is beneficial, but it's not always required. To be successful in this position, a person needs a solid understanding of networking or system administration, attention to detail, patience, and problem solving and task management skills.

Cybersecurity Consultants

Cybersecurity consultants provide a wide range of services and require an extensive background in security. Essentially, they're tasked with providing security expertise to an organization for whatever task or problem the organization is currently dealing with. This includes issues such as policy creation, system security controls, incident response, training and awareness, and general security advice. Consultants require a deep understanding of the overarching principles of security and typically have a base knowledge of most operating systems, software, or specific hardware devices. Critical thinking, problem solving, excellent verbal and written skills, and task management skills are essential for this position.

Cybersecurity Architects

We typically think of an architect as someone who designs buildings. A *cybersecurity architect* has a similar job, but instead of buildings, they design security. They're tasked with creating security controls for environments rather than implementing or managing existing controls. This means they must have a complete understanding of how security controls work and of the environment they're working with, as well as how that environment and the controls within it interact during normal workflow. For example, a network security architect would design the security controls that protect a particular network environment, taking into account the security devices needed, how information flows across the network, and any necessary network security controls on individual systems.

If you think this sounds like a sizable and complex job, you're right. Cybersecurity architects must have a vast amount of experience in their particular area of expertise, such as networking or databases, in addition to a robust security background. Understanding what controls a workflow needs and how those controls might have adverse interactions with other parts of an environment requires high-level critical thinking and problem solving skills. Architects must also work with diverse teams that span every aspect of IT, so they must hone their written and verbal communication skills. Additionally, architects are often working against a production timeline, which means they need to be efficient but diligent in their work.

Chief Information Security Officers

Organizations generally have a group of people tasked with running all operations. These people hold titles such as chief executive officer (CEO), chief financial officer (CFO), or chief information officer (CIO). In the security sector, the comparable position is the *chief information security officer (CISO)*. The CISO oversees all security operations within an organization:

they make broad decisions about how the organization should manage its security and what projects or resources the company needs to ensure it maintains an adequate level of security for the threats it faces.

The CISO requires an extensive understanding of security, but what sets them apart from most security professionals is their other skills. To be a CISO, you need excellent project management skills and budgeting experience. You also need to be able to communicate with your team and other executive officers to explain the organization's goals and mission, as well as how security relates to them. CISOs spend a good amount of their time as managers, whether with respect to personnel, budgets, or risk. Risk management requires you to identify a threat, the impact of that threat on the organization, the likelihood of that threat being realized, and what you can do to mitigate it (Chapter 10 covers risk management in depth). As the head of security for your organization, strong leadership skills are also a must.

Even small organizations need a CISO. Having a person in this role, whether it's a full-time job or part of other duties they carry out, is integral to building and maintaining security. Smaller organizations might consider finding a consultant to provide CISO-level guidance on a part-time basis.

CYBERSECURITY SPECIALTY AREAS

Although many careers in cybersecurity require a diverse knowledge of information technology, there are also many specialty areas that focus solely on one type of system or environment. For example, if you're a network administrator with a background in Cisco hardware, you might focus primarily on network security. If you're interested in malware, you might focus on malware analysis. Keep in mind that focusing on a specific area doesn't mean you can ignore security concepts related to other areas. Having a broad understanding of security in general will help reinforce the skills you learned for your particular area of expertise.

Incident Responders

An *incident* is anything bad that happens to an organization: for example, an account is compromised, data is lost or destroyed, or malware has infected a system. *Incident responders* are the people who react when an incident happens. Their main job is to run an initial investigation, preserve information and evidence, contain the incident from spreading, and restore affected systems as quickly as possible. You can compare an incident responder to a paramedic. Paramedics stabilize an injured person and determine how they were hurt so the doctor can fully treat them. Incident responders are somewhat similar: they don't perform the full investigation into what happened. That is left up to forensics experts, which we'll look at shortly.

Instead, incident responders stabilize the systems where the incident occurred to ensure the attack doesn't spread across the entire environment.

For example, they might take a system off the network to stop the spread of malware. Incident responders then gather and preserve evidence of the incident. This means checking logs, copies of systems, backups, and whatever other information they can find. Once they've gathered all the data and have the incident contained, they work to restore the environment. This might mean wiping a system to remove any possible trace of malware, for example.

Incident responders must work quickly but methodically. They require a cool head under pressure. They must be critical thinkers capable of reasoning through every action to ensure they don't make the incident worse or destroy evidence. Incident responders usually have a strong security background but often require additional training in specific incident response techniques. Responders typically work in a large team. Often, they're called on to provide specific system expertise for that team; for example, they might have an in-depth understanding of Linux operating systems.

Vulnerability Managers and Threat Hunters

Whereas incident response is about reacting to a harmful occurrence, vulnerability management attempts to prevent adverse events before they happen. *Vulnerability managers* look for security flaws in systems and try to correct them. This is a constant process, because systems continuously change and thus develop new vulnerabilities. A vulnerability manager needs patience and diligence, leaving no stone unturned to ensure they leave no vulnerabilities undiscovered.

Threat hunters have similar jobs, but they operate on a deeper scale, attempting to correlate events from across an organization to detect possible threats. They often look for advanced black hat activity, such as that carried out by an APT and not normally identified by typical alerts. Threat hunters require deep security knowledge, an eye for details, and excellent critical thinking skills. They also need good verbal and written communication skills to inform everyone in the organization about the threats they're detecting.

Computer Forensic Analysts

After an incident takes place and incident responders have completed their job, the forensic analysis of the incident begins. *Computer forensic analysis* is the process of retrieving and analyzing evidence related to an incident.

Computer forensic analysts could be part of the incident response team but are often a separate group that takes over the investigation after the threat has been contained. These analysts do a deep and detailed investigation of the evidence gathered. Not only do they look at items like logs, but they also examine the processes that were running on a system, what was loaded into memory during the incident, and even individual software code. This requires an extremely technical background with an in-depth knowledge of the inner workings of computer code. Computer forensic analysts use a variety of specialty tools that require training and practice to use effectively. They must have an intense attention to detail, as well as good communications skills to relay their findings in language accessible to nontechnical people.

Penetration Testers

The quintessential role for most people with cybersecurity expertise is *penetration tester*. They try to break into a system as if they were black hats to discover the system's flaws and vulnerabilities. Penetration testing is actually a minor field that requires a great deal of training to be successful.

Penetration testers must have robust technical skills, because they must understand security concepts and the types of techniques attackers use. This requires constant training and practice. Penetration testers rely on a variety of tools to attack systems, each of which comes with its own set of expertise. It's also essential that they maintain meticulous documentation to provide evidence of their actions to the client: ultimately, breaking into a system doesn't matter if you can't explain how you did it.

Exercise: Learning More About Cybersecurity and Threats

To better understand cybersecurity, it helps to get involved in the community. The best way to do this is to sign up for newsletters and alerts. The following sections provide a list of some of the best feeds available to get you started. As you look through these resources, try to answer these questions: What types of threats are most common? How do various sources categorize these threats? What common advice can you find across different resources to prevent attacks? What sorts of search terms might you use to find more resources?

Government resources

National Institute of Standards and Technology (NIST) Computer Security Resource Center at *https://csrc.nist.gov/* : a great place to find articles and other information on how to secure your systems at home or work.

Cybersecurity and Infrastructure Security Agency (CISA) at *https://www.cisa.gov/* the government agency charged with providing guidance on cybersecurity and infrastructure security. The site contains lots of resources and bulletins on security practices and threats.

National Institute for Cybersecurity Education (NICE) at *https://www.nist.gov/itl/applied-cybersecurity/nice/*: part of NIST, this group provides educational resources related to cybersecurity, including challenges and training courses for middle and high school students.

Threat feeds

Multi-State Information Sharing and Analysis Center (MS-ISAC) at *https://www.cisecurity.org/ms-isac/* this site provides alerts on critical vulnerabilities and other information related to cybersecurity.

InfraGard at *https://www.infragard.org/* this program provides national and state organizations with threat intelligence as well as other services, including training.

SANS Internet Storm Center at *https://isc.sans.edu/* this site provides updates on security vulnerabilities and blog posts on various security topics.

Cybersecurity blogs

Krebs on Security at *https://krebsonsecurity.com/* written by security expert Brian Krebs, this site provides lots of informative articles on current threats and other cybersecurity trends.

Threatpost at *https://threatpost.com/* this site provides articles on the latest vulnerabilities and threats being exploited.

FireEye Blogs at *https://www.fireeye.com/blog.html*: this site contains information on threats, stories from the industry, and other valuable cybersecurity articles.

Cybersecurity podcasts

Security Now at *https://twit.tv/shows/security-now/*: hosted by Leo Laporte and Steve Gibson, this cast delves deeply into the headlines of the week related to cybersecurity. It's a great resource to use to keep up with the latest vulnerabilities, exploits, and threats.

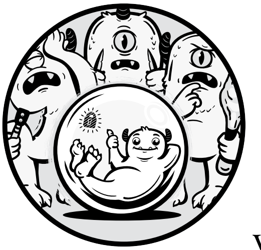
Darknet Diaries at *https://darknetdiaries.com/*: created by Jack Rhysider, this cast investigates real-life stories of hackers and other security events over the years.

Conclusion

Cybersecurity can be an intimidating field to enter. However, faced with a wide variety of attackers and threats, organizations need cybersecurity professionals more than ever if they want to preserve their security. This chapter introduced you to what cybersecurity is and the threats that exist. The rest of the book will guide you through the cybersecurity field and the threats you might encounter, whether you're a manager, a long-time IT person switching to a new field, or someone just entering the professional world.

2

ATTACK TARGETS ON THE INTERNET



You know what types of black hats exist, but a question still remains: how do they find you? Most people don't expect to be targeted by an attacker. You might wonder what you have that a black hat wants.

You'd be surprised at what an attacker finds valuable. It's true that many steal credit card and social security numbers, but others look for more than just personal data. Some might want information about other targets. Or they might want access to your equipment, such as computers or routers, to carry out other hacks. They might even be looking for insecure devices, just to have a little fun. In these cases, any device that is connected to the internet becomes a target for black hats.

We all have plenty of devices, some we might not even know about, that use the internet and need to be secured against black hat attacks. In this chapter, we'll briefly look at how the internet works, including a history of the technology, to help you better understand how an adversary uses it. Next, I'll break down how black hats prepare an attack with the information they gather from public resources. I'll finish the chapter by explaining how to hide from attackers by implementing three essential rules of internet use.

How the Internet Works

To comprehend how a black hat finds and exploits you on the internet, you need to understand some fundamental concepts about how the internet works. The internet as you know it today began as a project in the *Advance Research Projects Agency (ARPA)*, a United States government organization tasked with researching new technologies to maintain a lead over the Soviet Union.

In the 1960s, ARPA began working on a tool that would protect US communications during a nuclear attack. Because nuclear bombs could easily wipe out massive amounts of infrastructure, the US military needed a communications network that could reactively realign itself should part of the country be attacked. For example, if Washington, DC, was hit with a bomb, the military needed to be able to bypass the communication lines that went through the city so it could continue to share information with other parts of the country seamlessly.

One solution to this problem was the idea of *packet switching*. The premise was to put information into packets, or self-contained units, and then have a computer decide in real time where those packets should be sent based on information provided to it. For instance, if a computer received a packet destined for Atlanta (identified by an address attached to the packet) and knew that the intermediary Washington, DC, communication lines were down, it could automatically send that packet to, say, Cleveland, which could then pass it on to Atlanta. This allowed computers to create and maintain a network of communication even if part of the network was destroyed.

ARPA and many other researchers worked on implementing packet switching in large networks. Until that point, devices had communicated with each other directly via dedicated circuits set up between them. A circuit was typically a single physical line, and any break in the line would bring down the entire network. By the late 1960s and early 1970s, several smaller networks, created mostly to communicate between various universities and supercomputer sites, used packet switching to allow computers to communicate with each other over vast distances. Figure 2-1 shows a breakdown of the sites connected as part of *NSFNET*, one of the early networks that would later become the internet. This work continued into the 1980s, when commercial desktop computers become more readily available to the public.

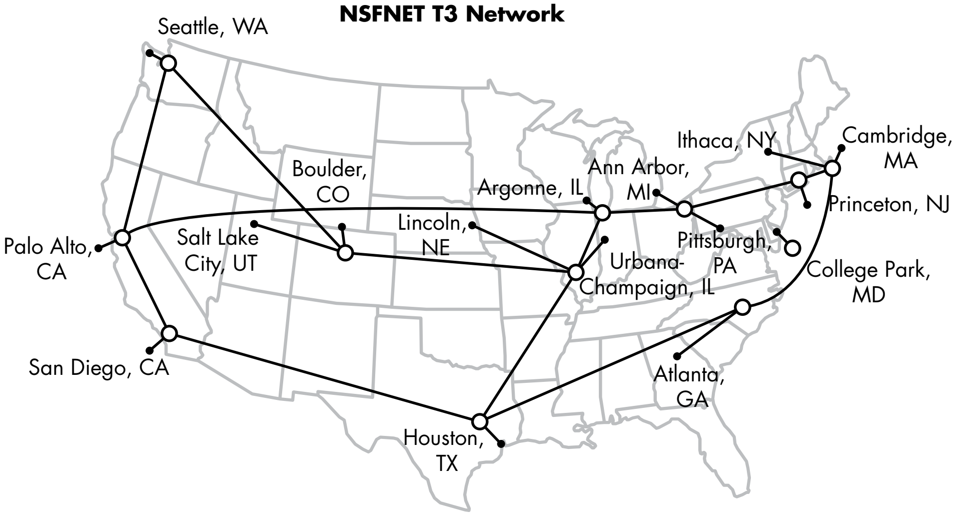


Figure 2-1: NSFNET in 1992, connecting various academic and other sites across the United States. (image altered from the original created by Merit Network, Inc. under the Attribution-ShareAlike 3.0 Unported [CC BY-SA 3.0] license, https://creativecommons.org/licenses/by-sa/3.0/deed.en*)*

It was also at this time that Robert Kahn and Vinton Cerf first developed the communication protocols known as the Internet Protocol (IP) and Transmission Control Protocol (TCP).

TCP/IP: The Backbone of the Internet

TCP/IP (sometimes referred to as the *IP suite*) is the set of protocols that runs the modern internet. Protocols are special codes that define how a system should understand and process the data received over a network. For example, the HTTP protocol tells a system that the data sent is a website and should be processed by a web browser. The TCP/IP protocols tell systems how traffic (flows of data) should be passed from device to device to reach a destination. It's part of the information that systems use to make adjustments in a packet-switching network.

The IP protocol provides a number, known as an IP address, that identifies the location of a computer on a given network. You can think of an IP address as your ZIP code. A ZIP code identifies a general region that the postal service uses to direct a package. There are two versions of IP addresses, version 4 (called IPv4) and version 6 (called IPv6). In this chapter I'll only discuss IPv4, because it's still the most common.

TCP is a set of rules that allows one system to communicate with another system while ensuring that both systems are available on the network. TCP is essentially the same as calling a friend to confirm they'll be home to receive a package when it comes in the mail. We'll talk more about these two protocols in Chapter 6.

With TCP/IP, packet-switching technology, and cheaper home computers, it didn't take long before commercial companies became interested in setting up their own networks so businesses and homes could communicate. Eventually, these networks began mingling, connecting larger and larger numbers of systems until the internet evolved naturally to consist of internet service providers (ISPs). ISPs, such as AT&T, Comcast, and Verizon, began to provide internet access and sell the necessary infrastructure to businesses and eventually homes. Since the early 1990s the world has become more interconnected, with computer networks reaching nearly every corner of the planet.

Public vs. Private Networks

Today's internet is made up of a large number of connected smaller networks. These networks can generally be categorized into two types: public and private. Essentially, anyone can use a *public network,* usually by paying a fee. For example, the network that your house connects to and that you pay an ISP to use is a public network. These form the backbone of the internet, because they allow any paying customer to connect. Often, public networks are run by ISPs.

Frequently, public networks are also connected to *private networks,* which only allow connections to a limited group of devices. For example, if you work in an office, you might be able to access files from a specific server through a connection from your desktop computer. The server and the desktop computer are on a private network, meaning they're only allowed to communicate with each other or other devices on the private network. People on the public network (the internet) can't directly see, connect, or access anything on the private network.

Many private networks have a connection to the public network through equipment provided by an ISP, and they pay to get access to the internet. For example, your home might have a Wi-Fi network. Only the people who live at your house or guests to whom you give access can use that Wi-Fi network, making it a private network. However, your house is connected to the internet, usually through a special device called a *modem* or *router.* These devices pass your traffic between your home Wi-Fi network and the ISP's public internet. You, along with people in your neighborhood, pay the ISP to access the internet using special ISP equipment. Without you letting them have access, people can't just access your private network from the public network.

Figure 2-2 shows how the internet with its public and private networks might look as a visual map. Billions of *nodes* make up the internet. These nodes represent connections between IP addresses. The expanded section in the bottom-right corner of the figure reveals how individual addresses, such as 207.205.290.168, are connected to an ISP to form larger connections that create the internet.

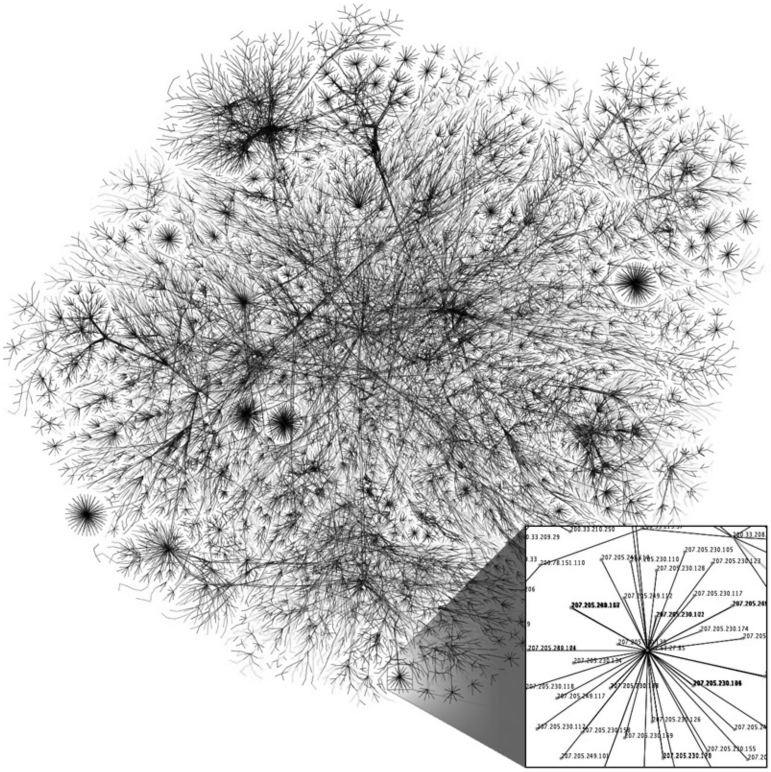


Figure 2-2: A map of the internet. (image altered from the original created by the Opte Project under the Attribution 2.5 Generic [CC BY 2.5] license, https://creativecommons.org/licenses/by/2.5/deed.en*)*

Private and public networks are differentiated by the type of IP address they use. An IPv4 address is made up of four numbers, each ranging from 0 to 255, usually separated by periods: 192.168.15.1 and 10.10.10.255, for example. Certain ranges of those numbers are set aside for use by private networks only, whereas the rest are available for the public. Private addresses use certain addresses that never change, such as 10.0.0.0 or 192.168.27.0. Public addresses get translated to private addresses when you connect from a public network to a private network, and vice versa. For example, when you connect to google.com, you might connect to the address 8.8.8.8 (a public address). Once the connection to 8.8.8.8 is made, Google's own network equipment might translate that connection into a private address, such as 192.168.1.1, so you can access resources on Google's private network. This process is known as *Network Address Translation (NAT).*

How the Internet Looks to a Black Hat

When a black hat accesses the internet, they're often trying to figure out how they can get past the public network and look into a private network.

This can be exceedingly difficult, because many of the systems that make the internet what it is today are designed specifically to prevent people on a public network from seeing what's going on in any private network. Consider the NAT process: the person connecting to the public address doesn't see the translation or what is happening behind the scenes. When you connect to google.com, you connect through a web browser, and the Google website appears. You're not informed of and normally can't see all the mechanisms on Google's private network that allow the web page to operate the way it's supposed to.

So when an adversary focuses on a target, their first step is often to determine how they can move from the public side of a network to the private side. Once they're in the private network, they can work on finding their specific target and executing the attack to get whatever they're after, whether that's disrupting business as usual or stealing data. To perform all these actions successfully, many black hats rely on a certain set of steps to maximize their attack's potential.

The Black Hat Attack Methodology

Not every attack by a black hat follows a specific pattern or set of steps. But most attackers must accomplish certain objectives before they can fully realize their goals. Several models classify these objectives, but one of the most famous is the *Lockheed Martin Cyber Kill Chain (CKC)*.

The CKC consists of seven steps that a black hat must accomplish for their attack to be effective. These steps involve activities undertaken before, during, and after many cyberattacks: they include *reconnaissance*, *weaponization*, *delivery*, *exploitation*, *installation*, *command and control*, and *attack on objectives*. Let's look at each step in more detail.

Reconnaissance

During the reconnaissance phase of the CKC, the attacker learns everything they can about their target. They begin by collecting any data considered public information. In the case of an organization, this means data from their websites and social media, as well as data about their employees, their organizational structure, physical locations, groups they've partnered with, recent news stories, public IP addresses owned by the organization, and more. For an individual, this might include information about their family members, where they work, where they live, criminal and other government records, and of course, social media.

These adversaries also look for not-so-public information, much of which is still available on the internet if you know where to look. This includes websites that, although accessible by everyone, might not be meant for public consumption, such as an employee's remote login page. Or it might include details collected about a public IP address, such as the services it's running. The black hat might also begin listing relevant email addresses by mining social media or other places on the internet to use at a later time.

One of the ways that attackers can find information is by sniffing and scanning. *Sniffing* is intercepting and analyzing other users' network traffic. Black hats can do this without interrupting the traffic flow, so the user remains unaware that their traffic is being monitored. For example, an attacker might look at all the data coming from an email server and copy any attachments before sending the original emails to their destinations. *Scanning* is sending specially crafted packets to a device and listening to how it responds to those packets. The responses can provide the black hat with information about what kind of system or software the node is running. For example, if an attacker wants to know whether a host is running a Windows operating system, they can send a packet made specifically for a Windows system. If the system responds with an error, they know it's not a Windows system. We'll talk more about scanning and sniffing in "Attacking Your Network" in Chapter 6; both can be lucrative sources of information for an adversary.

All of this reconnaissance work provides information that helps black hats narrow their field of focus until they know where to begin their initial attack. It also provides valuable information they can use in the next phase to craft attacks that are likely to work. For example, if an attacker scans a public IP address and finds it's connected to a Windows server, they won't waste time using Apple exploits on it. This is what makes reconnaissance such a key part of mounting a successful attack.

Weaponization

In the next step, weaponization, the black hat creates an actual attack to use against a target. With the information gathered from the reconnaissance phase, they plan and create the tools they'll need. This phase also requires that the adversary have a good sense of what will get them to their mission objective the quickest. For example, if the attacker's objective is to gather more personal information about a target and use it to blackmail them, they might try to exploit the target's email. Creating a virus that destroys Word documents, although an effective attack, wouldn't be a great way to meet this objective. Instead, it's a much better idea to create a PDF that links to a fake email login page and try to trick the victim into using it. That way, the attacker may be able to gather the victim's credentials from the fake page and use them to log into the legitimate account.

Delivery

Once the black hat has a weaponized package, whether it's malware, a phishing website (which we'll discuss in more detail in Chapter 3), or some other form of attack, they're ready to deliver. Again, this requires using the information gathered during the reconnaissance phase to decide what the best method of delivery will be. Many recent attacks have been delivered through email, but this might not always be the best method.

If the attacker knows that the target uses a device with a known flaw, they might craft a delivery method that takes advantage of this flaw. For example, if a company website was using a fillable form that included exploits, an adversary might be able to inject code directly onto the web server through the exploit. This would allow them to deliver their attack directly to the server instead of having to rely on an employee to install it for them.

Exploitation and Installation

The next two steps, exploitation and installation, rely on getting the exploit installed once it's delivered. This means getting a person to click a malicious link or launch the malware created during the delivery phase. Once the exploitation is done, the black hat should be able to execute their attack or install malware on the device.

Keep in mind that many of the items attackers want, such as credit card numbers or other personal information, are usually stored on private networks, inaccessible to the public. This means that attackers must compromise the private network before they can fully access it.

This compromise usually involves the adversary establishing *backdoors*. Consider this analogy: if the front door is the way people are supposed to enter a house, then using the back door (or garage door) would be a way for someone to bypass the controls, such as the lock on the door. Black hat backdoors work in a similar fashion, allowing an adversary to access the system without having to go through the normal, trusted means of authentication.

Command and Control, and Attack on Objectives

During the command and control and attack on objectives phases, the black hat uses the backdoor to establish a foothold in the system. From there, they can use it as a base to identify further systems to exploit. This is known as *pivoting*. Attackers will continue to pivot until they can reach their objective directly (as discussed in Chapter 1, objectives will vary depending on the type of attacker). Once they find a way to their objective, the attacker will launch a full set of attacks to gain access and accomplish their mission.

The command and control phase involves creating a command and control server, which is a tool that allows the attacker to send the compromised device commands from a remote location and receive information. For example, if a black hat compromises a web server, they might instruct that server to reach out to other devices on the network to find additional systems they could compromise. Often, these commands use normal traffic patterns to hide, so it's harder for white hats to detect them until it's too late.

The attack on the objective is usually done in a similar stealthy manner to ensure that the black hat isn't prevented from getting what they want and that the organization can't mitigate the damage. If an attacker steals a number of credit card numbers, they're only useful if the bank doesn't know they've been stolen, at which point it would cancel them before they can be sold or used. With this final phase complete, the black hat sells their prize and moves on to the next target, again starting at the reconnaissance phase.

How Black Hats Find You

If you look closely at the phases of a black hat's attack, you'll notice that one of the most important steps is the first one: reconnaissance. If an adversary can't find any useful information about their target, they'll have an extremely difficult time delivering an effective attack. This, of course, makes it that much harder to get a foothold in the private network.

So, where do black hats find their reconnaissance information? They find it mostly from publicly available sources, which people often create without realizing what they're exposing. Often, misconfigured systems openly communicate on the internet, exposing services that an organization might not want available to the public. You can see many of these open systems by using *Shodan*, a tool that scans the internet for open services and systems. After a scan, Shodan puts its findings in an easy-to-use database that is open to the public to search through. Using Shodan, you can find all sorts of detailed information on the types of devices that are publicly accessible from the internet. We'll walk through using the tool in the exercise at the end of this chapter.

Using Shodan isn't the only way to find useful information online. A ton of data on the internet might help a black hat craft an attack. Let's look at a few scenarios to help you understand how an adversary can gather this type of information.

Example 1: The Merger

Say an attacker learns that Sparkle Kitten Inc. is buying Smelly Puppy Co. and merging the company directly into Sparkle Kitten. By reading the news, the black hat learns that the CEO of Smelly Puppy is unhappy about the merger. The attacker decides to target Smelly Puppy during this stressful time. They begin by scanning Smelly Puppy's website to look for any listed email addresses. By using an automated tool to comb through all available web pages, even those that might not be available via a Google search, they locate a job ad for an administrator with knowledge of a specific type of web server.

Using public registration information, the black hat can find exactly which IP addresses the company bought and registered to use. The adversary then uses a scanning tool that targets those addresses, looking for that particular web server. They find the server, and what's more, discover that it responds to the traffic sent to it. Now they can craft an effective attack using a known exploit and gain access to the server.

Example 2: Social Media Hunting

A black hat wants to gain access to Secure Co., one of the most secure companies in the world (it says so in its name). The attacker knows that Secure Co. uses the latest appliances, training, and best practices to remain secure, because Secure Co. advertises this information often. The black hat also realizes the organization uses a specific marketing company, Super Awesome Marketing, for all its advertising. The adversary decides that instead of attacking Secure Co. directly, they'll attack Super Awesome Marketing.

To do so, the attacker looks through LinkedIn and Facebook to find employees who work at Super Awesome Marketing. They locate a particular employee who works for the IT department and track them on Twitter. Every morning, this employee takes a picture in the same gym. The black hat also notices they leave geolocation tags on their posts. Using those tags, the black hat finds the gym the employee uses. The attacker visits that gym one morning, listens to the employee's conversations, and hears about a particular exploit in Super Awesome Marketing's email server. The adversary uses that exploit to gain access to the email server, where they can then take over an employee's email account. Now the black hat has a means of infecting the marketing material Super Awesome Marketing creates for Secure Co. Because this material is coming from a trusted vendor, it proceeds right past the normal security checks and stealthily sets up a backdoor inside Secure Co.'s private network. Not so secure now, huh?

How to Hide from Black Hats

The previous examples on how an adversary gathers information might seem far-fetched, but they describe real-life techniques that black hats have used. When people post information publicly, attackers can use it to find cracks in their security, allowing the attackers to craft the perfect attacks against a person or organization. The best way to defend against these attacks is to implement *operational security (OPSEC)*.

OPSEC is the process of understanding and minimizing any information that could be used against you. The technique originated in the military, which worried about tipping off an enemy about an attack by revealing seemingly noncritical information. For example, if the military moved a unit to a new base, an opponent could correlate this action with other information to deduce that the military was planning an attack on a certain country, perhaps one that was closer to the new base.

For civilian organizations, OPSEC is about protecting information that a black hat could use to attack your organization. This means limiting the information you share on a public website, press release, or social media. OPSEC is tricky to get right, because it's difficult to know what an attacker might find useful in the right context. The best way to ensure your OPSEC is to keep three rules about the internet in mind when posting information: the internet is open, public, and forever.

The Internet Is Open

When you're using the internet, assume that anyone can see what you're doing or sharing, including any data moving across the network. It's up to you to protect that information by determining how you send it.

A good example is the ability to request web pages. When you access a web page, your browser has to figure out where that page is located on the internet. It does this by querying a *Domain Name Service (DNS)* server, which contains records of the public IP addresses to which websites are assigned. For example, a DNS server might tell you that the domain sparklekitten.net is at the IP address 1.1.1.1. When you tell your browser to go to sparklekitten.net, it sends out a request that eventually ends up at the DNS server, which provides the record of the IP address where you can find sparklekitten.net so your browser can access that website.

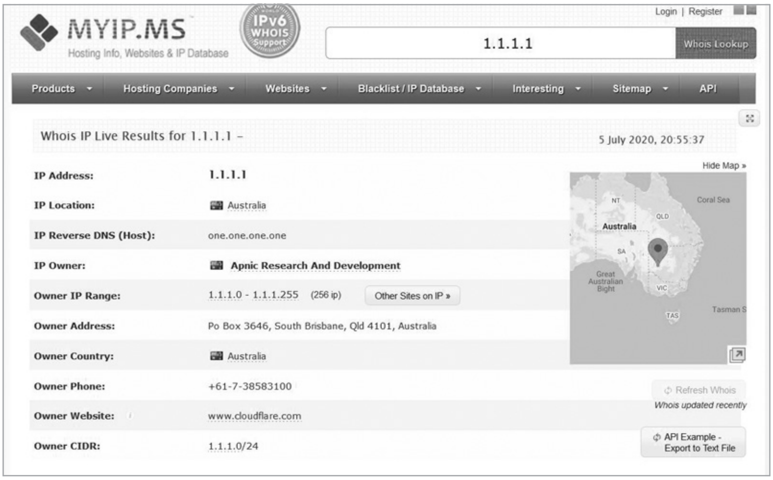
Usually, DNS requests travel through a series of DNS servers until they find the right one. Your browser starts by sending a request to a server, hosted by your ISP, which sends it to another DNS server, which sends it to another, until it finds the Sparkle Kitten DNS server with the correct record. Until recently, browsers sent these requests almost entirely unencrypted, meaning they remained in plain view for anyone to see. So not only could your ISP see every web page you requested—information it was more than willing to sell to marketing firms—but anyone with the ability to sniff your traffic could also see your DNS requests. Even if you were using a private browser or visiting websites using encrypted links, that DNS request used unencrypted protocols, so anyone could know which website you were trying to reach.

Fortunately, many browsers have since begun supporting DNS requests sent over encrypted links. Still, this is a prime example of how the internet is open. As you browse, send email, or download files, you're relaying information that is being cataloged, stored, and often sold. This information can easily be exploited to learn about you or your organization to craft the perfect attack. This is why it's important to be mindful of the kind of information you communicate on the internet. Although you don't need to cut yourself off from the world entirely and live in a cave, it's best to ensure you encrypt any sensitive information, especially if you send it through email, file sharing, or social media. It's frequently a good idea to research the services you use and what data they might be collecting on the backend. Even though it might take additional time and effort to take these steps, the extra security and peace of mind they offer is more than worth it.

The Internet Is Public

The internet is completely public; anyone can get online as long as they have the right connection set up or pay a company, like an ISP, to use their equipment. In many ways, access isn't even tied to a specific person. It's possible, legal, and often best to hide who you are on the internet by using usernames or hiding your IP address (more on this later). This applies not just to usernames on a video game or social media site, but also to your IP address and your physical location in the world.

One way to track down an IP address's location is to look up the registration information using a *Whois* search. Whois is a database of website registration information. Several websites provide Whois information, including Myip.ms, shown in Figure 2-3 displaying the Whois record for the IP address 1.1.1.1.



Whois IP Live Results for 1.1.1.1 – 5 July 2020, 20:55:37

IP Address:	1.1.1.1
IP Location:	Australia
IP Reverse DNS (Host):	one.one.one.one
IP Owner:	Apnic Research And Development
Owner IP Range:	1.1.1.0 - 1.1.1.255 (256 ip)
Owner Address:	Po Box 3646, South Brisbane, Qld 4101, Australia
Owner Country:	Australia
Owner Phone:	+61-7-38583100
Owner Website:	www.cloudflare.com
Owner CIDR:	1.1.1.0/24

Figure 2-3: 1.1.1.1 Whois record

Although public IP addresses are tied to specific regions in the world, it's very difficult to trust that the person using an IP address is actually present in that location. Just like you can translate public IPs to private IPs, you can translate a public IP address to a different one. This can make it difficult to track down where traffic is actually coming from, which allows a black hat to easily hide in plain sight.

This also means that people from other countries, your teachers, your grandmother, or even your postal worker can access what you post on the internet. More importantly, if you put something on the internet and make it public, it can be difficult to stop people from seeing it. Even if you think you're only sharing something with your friends, it's possible that your friends are sharing it with the public at large. The best rule to adhere to when posting any information to the internet is to assume that everyone will be able to see it, so craft what you say with that assumption in mind. If you think the post might hurt you or provide information that others can use against you, it's best not to post it in the first place.

The Internet Is Forever

It's nearly impossible to delete information from the internet. For instance, when you delete an email, is it actually gone? If you're using a service like Gmail, deleted mail goes into a trash folder, which holds it for 30 days before it's removed from sight. So the email you deleted isn't really deleted; it's just placed in a different place where an adversary could still access it.

In the case of social media, the situation is even worse. Companies like Facebook and Google make a lot of money from the data people create on their platforms, so it benefits them to hold on to it for as long as possible. Facebook and Twitter store posts for many years. Even when you remove yourself from the platform, posts you've made in groups that you were a part of remain publicly available. Try googling your full name and state; you might be surprised to find your posts in the search results.

Also, many people document online activity to keep a record of the internet as it changes. One of the main projects doing this work is the Internet Archive, at *https://archive.org/*. The Internet Archive attempts to catalog every web page created, so even if you've removed or edited web pages, it's possible a record of them exists for people to find.

Just as it's important to assume that everyone can see what you post on the internet, it's just as important to assume that your internet posts will exist forever. Again, this doesn't mean you should forgo using the internet entirely. Just be mindful of what you do when you're online.

Understanding the three rules of the internet will help you practice OPSEC if someday you work for an organization that needs to prevent sensitive information from becoming public. By being mindful of how you post your personal information, you'll notice information that black hats could potentially use to attack your organization. You could also teach others in your organization, especially new hires, about the importance of limiting the information they share with the public. This behavior will make your organization more secure overall. After all, the less information an attacker has, the harder it is for them to attack.

Exercise: Analyzing Your Network

As you learned in this chapter, it's important to understand the information you're posting to the internet. Otherwise, attackers might use a post you've unknowingly left visible to access your accounts or your private network. As mentioned earlier, you can use Shodan to find this information, which, as you'll recall, is like a search engine for IP addresses.

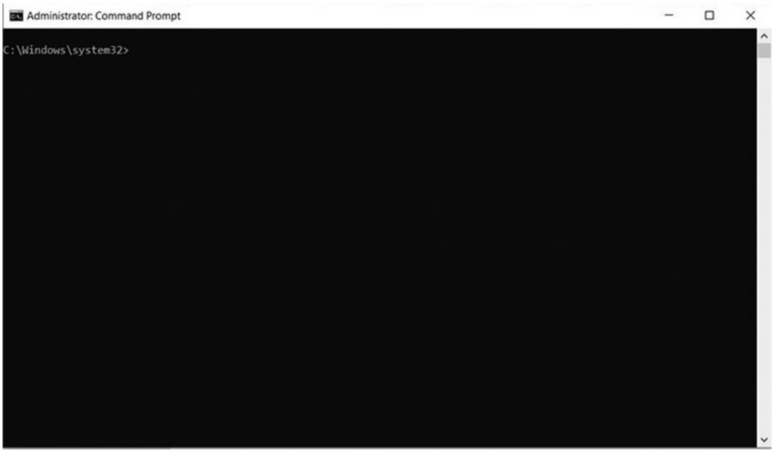
Although you can use Shodan in your web browser, other useful tools require the *command line*, which allows you to enter commands on your system to perform tasks. In this exercise, you'll learn how to use some of these simple commands to discover information about your network. Then you'll use that information to search Shodan to see what sorts of services you're leaving open on the internet.

Network Command Line Tools

Windows and macOS operating systems come with built-in tools that can help you learn about your network. Let's look at four of these tools that are particularly useful for finding information that you can then use when searching with Shodan. Before you can begin using commands, you'll need to access the command line on your system. Windows and macOS have different command line programs; each uses slightly different versions of the commands and has different outputs. Let's look at them separately.

Windows

Locate the search bar in the lower-left corner of the screen and enter **CMD**. At the top of the results, you should see an app called *Command Prompt*. Select it, and a window like the one in Figure 2-4 should appear on your screen. If you're not running as an admin, the text after C: will be your home directory and include your current username.



```
C:\Windows\system32>
```

Figure 2-4: The Command Prompt window

First, we'll use the `ipconfig` command. This command outputs your current networking configuration, including your computer's assigned IP address, its default gateway, and information about your DNS server. The default gateway is the first router to which your computer connects to transmit traffic out of your network. Routers pass traffic from one to another to connect two endpoints together. A router creates a single network, which devices can join. So, the default gateway address is the address your computer needs to know to send traffic to the router that controls the flow of traffic into and out of your network. When you enter **`ipconfig`** in the Command Prompt window, you should see output similar to the following:

```
C:\Windows\System32> ipconfig
Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 10:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : lan
   Link-local IPv6 Address . . . . . : fe80::4d78:5074:4095:fe97%18
   IPv4 Address. . . . . . . . . . . : 192.168.86.36
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.86.1
```

```
Ethernet adapter Bluetooth Network Connection:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

Notice the section labeled `IPv4 Address` below `Wireless Lan adapter Wi-Fi`. This is your computer's private IP address. From this output, you can see that this system was assigned a private IP address. Also notice the section titled `Default Gateway` two rows below the `IPv4 Address` section. This identifies the router to which your system sends its traffic to leave the private network. In home networks, this is often the modem or router that the ISP provides. The default gateway also has a private IP address.

Although `ipconfig` gives you great information on what address your computer is using to communicate on your local network, it doesn't help you if you want to use Shodan, because you'll need to search for a public IP address, not a private one. You can use online tools to discover public IP addresses, but we'll use the `nslookup` command because it's another command line tool that is usually available. This tool looks up IP addresses assigned to website domain names. To use it, you'll need a target. For this exercise, let's use google.com. Run the command by entering **`nslookup`** in the Command Prompt window followed by **`google.com`**:

```
C:\Windows\System32> nslookup google.com
Server:  testwifi.here
Address:  192.168.86.1

Non-authoritative answer:
Name:    google.com
Addresses:  2607:f8b0:4002:c09::8b
          2607:f8b0:4002:c09::65
          172.217.9.14
```

The output from `nslookup` shows the public IP addresses currently attached to google.com. This tool is useful when you're trying to determine the IP address attached to a website to figure out where suspicious traffic in your network is coming from. Your output might look different depending on where you're located and the current configurations Google uses.

Now that you have a public IP address, you can use another tool called `ping`. This tool sends a small packet of information to an IP address and then listens for the ping's destination to respond back with its own packet of information. This tells you whether or not you can communicate with the system, because the system can't respond if it can't receive the ping in the first place. You can try using `ping` against the public IP addresses that you discovered using `nslookup`. Simply enter **`ping`** followed by the IP address you want to target:

```
C:\Windows\System32> ping 172.217.9.14
Pinging 172.217.9.14 with 32 bytes of data:
Reply from 172.217.9.14: bytes=32 time=14ms TTL=116
Reply from 172.217.9.14: bytes=32 time=14ms TTL=116
Reply from 172.217.9.14: bytes=32 time=14ms TTL=116
Reply from 172.217.9.14: bytes=32 time=15ms TTL=116

Ping statistics for 172.217.9.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 14ms, Maximum = 15ms, Average = 14ms
```

As you can see, ping sends out four packets. Each packet is tracked by how fast it goes out and returns to its point of origin. The speed is so fast, it's recorded in milliseconds. In this example, each packet took approximately 14 ms. At the end of the command, the system provides a summary of how many packets were sent and received. If you're unable to reach a system, ping will show the packets as lost.

Let's use one last tool that will provide you with all the information you need to search with Shodan. You know you can reach Google's IP address because of the results from ping, but they don't tell you *how* your packets actually got to Google's system. To learn that, you can use the tracert tool, which sends packets to each router along the path between your computer and the destination you want your traffic to reach. These packets provide information about the stops (or hops) your traffic makes on its way to its destination, using a feature called *Time to Live* (*TTL*). Essentially, each packet is designed to make only a certain number of hops based on its TTL number. A hop is counted when the packet is passed by a router. Each time a router passes the packet of traffic along, the TTL number is reduced by 1. Once its TTL reaches 0, the packet returns information about the last router to receive the packet. The packet *dies*, so the last router to hear it sends a message to the packet's next of kin, or in this case, the device that initially sent the packet. The tracert tool summarizes all of these hops. Enter **tracert** in the Command Prompt window along with a destination IP:

```
C:\Windows\System32> tracert 172.217.9.14
Tracing route to dfw28s02-in-f14.1e100.net [172.217.9.14]
over a maximum of 30 hops:

  1     2 ms     2 ms     2 ms  testwifi.here [192.168.86.1]
  2     3 ms     3 ms     3 ms  Address Removed by Author
  3    12 ms    14 ms    17 ms  Address Removed by Author
  4    10 ms     5 ms     5 ms  71.154.103.34
  5    29 ms    23 ms    15 ms  cr2.dlstx.ip.att.net [12.122.138.122]
  6    17 ms    14 ms    14 ms  12.123.240.25
  7    23 ms    22 ms    13 ms  12.255.10.100
  8    23 ms    23 ms    22 ms  209.85.243.95
  9    17 ms    22 ms    14 ms  108.170.231.69
 10    19 ms    22 ms    15 ms  dfw28s02-in-f14.1e100.net [172.217.9.14]

Trace complete.
```

The output shows that the first hop made is to your default gateway (in other words, your router). From there, it takes another nine hops before your packet gets to its destination. Each hop represents a router, either on your local network or on the internet. Each hop is sent three packets to show an average of how long it took to move to that point.

Using this tool is an ideal way to determine the parts of your network or the internet where your transmissions might encounter trouble reaching a destination. It also gives you a good idea of the public IP address assigned to your computer by your ISP; this should be the first public address you see, because your traffic has to make this hop to gain access to the internet. In the previous `tracert` output, I omitted the second and third results, because they link directly to my home network. But in a normal `tracert` execution, you'd be able to see these addresses.

macOS

On macOS, open the Terminal app to access the command line. To do this, use the search bar at the top-right corner of the screen. Enter **Terminal** and click the application that appears. Now you can learn some useful commands to help you find information about your network.

On macOS, you can use commands very similar to the Windows 10 commands, although some require slight variations. For example, instead of using `ipconfig`, you'll use the `ifconfig` command on macOS. The `ifconfig` command provides the same information `ipconfig` does but with much more detail, as you can see in this output:

```
$ ifconfig
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
options=1203<RXCSUM,TXCSUM,TXSTATUS,SW_TIMESTAMP>
inet 127.0.0.1 netmask 0xff000000
inet6 ::1 prefixlen 128
inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
nd6 options=201<PERFORMNUD,DAD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
XHC20: flags=0<> mtu 0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
ether b8:e8:56:16:38:10
inet6 fe80::8ec:dd2e:36cc:b962%en0 prefixlen 64 secured scopeid 0x5
inet 192.168.86.93 netmask 0xffffff00 broadcast 192.168.86.255
nd6 options=201<PERFORMNUD,DAD>
media: autoselect
status: active
p2p0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 2304
ether 0a:e8:56:16:38:10
media: autoselect
status: inactive
awdl0: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1484
ether ee:57:a6:16:74:96
inet6 fe80::ec57:a6ff:fe16:7496%awdl0 prefixlen 64 scopeid 0x7
nd6 options=201<PERFORMNUD,DAD>
media: autoselect
status: active
en1: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
```

```
options=60<TSO4,TSO6>
ether 32:00:1e:74:20:00
media: autoselect <full-duplex>
status: inactive
bridge0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
options=63<RXCSUM,TXCSUM,TSO4,TSO6>
ether 32:00:1e:74:20:00
Configuration:
id 0:0:0:0:0:0 priority 0 hellotime 0 fwddelay 0
maxage 0 holdcnt 0 proto stp maxaddr 100 timeout 1200
root id 0:0:0:0:0:0 priority 0 ifcost 0 port 0
ipfilter disabled flags 0x2
member: en1 flags=3<LEARNING,DISCOVER>
        ifmaxaddr 0 port 8 priority 0 path cost 0
nd6 options=201<PERFORMNUD,DAD>
media: <unknown type>
status: inactive
utun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 2000
inet6 fe80::b740:b05f:b952:2490%utun0 prefixlen 64 scopeid 0xa
nd6 options=201<PERFORMNUD,DAD>
utun1: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1380
inet6 fe80::508:28d2:8ad8:65a5%utun1 prefixlen 64 scopeid 0xb
nd6 options=201<PERFORMNUD,DAD>
utun2: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1380
inet6 fe80::e0b5:18ed:6a4c:a999%utun2 prefixlen 64 scopeid 0xc
nd6 options=201<PERFORMNUD,DAD>
```

The `ifconfig` command returns a huge amount of information. Within this output, it can be hard to find your device's IP address. Look for `en0` (ethernet 0), which usually identifies your main network adapter. By default, your main network adapter is assigned your IP address.

The `traceroute` command on macOS is similar to the Windows `tracert` command. It follows the same syntax, entering the command and then a target you want to trace to:

```
$ traceroute 31.13.93.35
traceroute to 31.13.93.35 (31.13.93.35), 64 hops max, 52 byte packets
 1  testwifi.here (192.168.86.1)  2.753 ms  2.391 ms  1.938 ms
 2   REDACTED 2.349 ms  2.619 ms  2.141 ms
 3  REDACTED 13.995 ms  4.940 ms  4.207 ms
 4  71.154.103.34 (71.154.103.34)  5.964 ms * *
 5  cr2.dlstx.ip.att.net (12.122.138.122)  16.537 ms  17.924 ms  20.084 ms
 6  dlstx410me9.ip.att.net (12.123.18.177)  14.537 ms  15.603 ms  14.522 ms
 7  12.245.171.14 (12.245.171.14)  15.592 ms  17.718 ms  31.346 ms
 8  po104.psw04.dfw5.tfbnw.net (157.240.49.143)  14.118 ms  13.705 ms
    po104.psw02.dfw5.tfbnw.net (157.240.41.125)  23.049 ms
 9  157.240.36.39 (157.240.36.39)  18.651 ms
    157.240.36.135 (157.240.36.135)  17.058 ms
    157.240.36.37 (157.240.36.37)  18.979 ms
10  edge-star-mini-shv-02-dfw5.facebook.com (31.13.93.35)  14.644 ms  20.972
    ms  20.617 ms
```

The nslookup and ping commands are nearly the same on macOS as on Windows. One key difference is that on macOS, ping doesn't perform only four pings by default. Instead, it continuously pings a system until the user manually stops the command. This can be useful if you're changing configurations on a system and want to make sure nothing you're doing is obstructing network access. But in most cases, you'll want to limit the number of pings you send to four or five to avoid sending too many pings at once. You can set the number of pings to send using the -c argument, which is short for count:

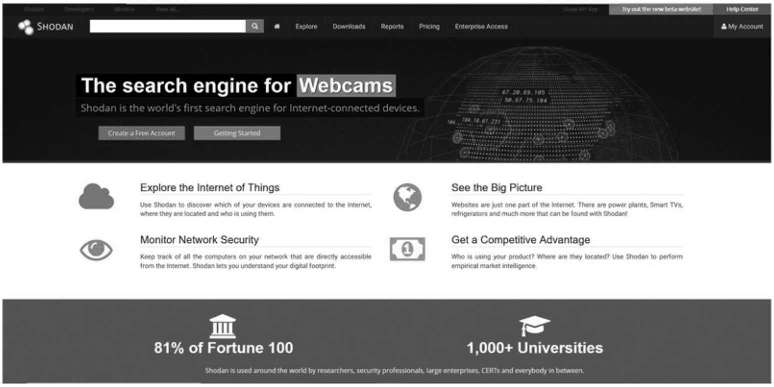
```
$ ping -c 4 192.168.86.1
PING 192.168.86.1 (192.168.86.1): 56 data bytes
64 bytes from 192.168.86.1: icmp_seq=0 ttl=64 time=1.891 ms
64 bytes from 192.168.86.1: icmp_seq=1 ttl=64 time=2.907 ms
64 bytes from 192.168.86.1: icmp_seq=2 ttl=64 time=5.073 ms
64 bytes from 192.168.86.1: icmp_seq=3 ttl=64 time=9.108 ms

--- 192.168.86.1 ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.891/4.745/9.108/2.769 ms
```

Using Shodan

Shodan comes in two forms: a command line tool you can install and a website you can browse through. For the purposes of this chapter, we'll look at the website only. You can access Shodan at *https://www.shodan.io/*. At the website, you'll need to sign up for a free account. The free account allows you to use most of the tool's functions, including searching through its databases, but it limits the amount of reports and other information you can download from the website. Figure 2-5 shows the home page.

Once you have a free account, browse through the website to become familiar with its layout. Start by clicking the **Explore** tab, which is just to the right of the search bar, near the top of the page. This page provides a breakdown of the various IP addresses Shodan has in its database and the services that are exposed on those addresses.



The search engine for Webcams

Shodan is the world's first search engine for Internet-connected devices.

Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

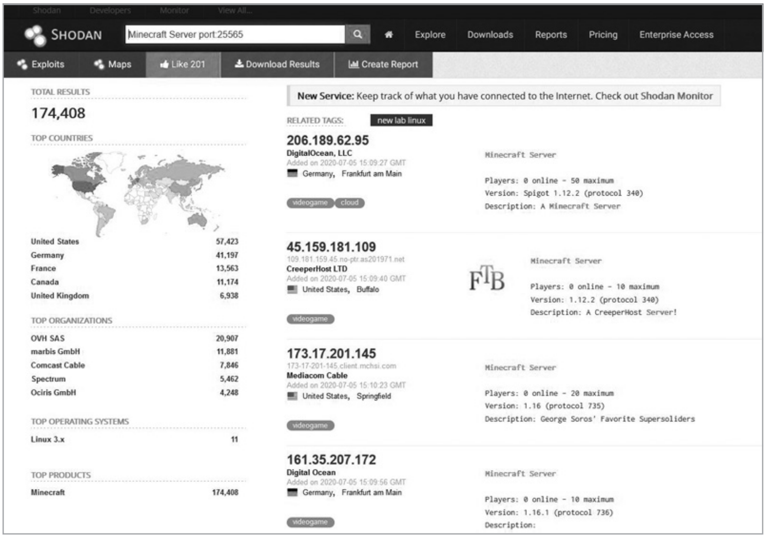
81% of Fortune 100

1,000+ Universities

Shodan is used around the world by researchers, security professionals, large enterprises, CERTs and everybody in between.

Figure 2-5: Shodan's home page

On the left side, you should see a few interesting categories. Click the one labeled **Video Games**. You'll see a list of various online games, including *Counter Strike*, *Starbound*, and *Minecraft*. If you click Minecraft, you'll get a rundown of all the open *Minecraft* servers currently located by Shodan. Figure 2-6 gives you an example of the list.



TOTAL RESULTS

174,408

TOP COUNTRIES

United States	57,423
Germany	41,197
France	13,563
Canada	11,174
United Kingdom	6,938

TOP ORGANIZATIONS

OVH SAS	20,907
marbis GmbH	11,881
Comcast Cable	7,846
Spectrum	5,462
Ociris GmbH	4,248

TOP OPERATING SYSTEMS

Linux 3.x	11

TOP PRODUCTS

Minecraft	174,408

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

RELATED TAGS: new lab linux

206.189.62.95
DigitalOcean, LLC
Added on 2020-07-05 15:09:27 GMT
Germany, Frankfurt am Main
videogame cloud

```
Minecraft Server

Players: 0 online - 50 maximum
Version: Spigot 1.12.2 (protocol 340)
Description: A Minecraft Server
```

45.159.181.109
109.181.159.45.no-ptr.as201971.net
CreeperHost LTD
Added on 2020-07-05 15:09:40 GMT
United States, Buffalo
videogame

```
Minecraft Server

Players: 0 online - 10 maximum
Version: 1.12.2 (protocol 340)
Description: A CreeperHost Server!
```

173.17.201.145
173-17-201-145.client.mchsi.com
Mediacom Cable
Added on 2020-07-05 15:10:23 GMT
United States, Springfield
videogame

```
Minecraft Server

Players: 0 online - 20 maximum
Version: 1.16 (protocol 735)
Description: George Soros' Favorite Supersoliders
```

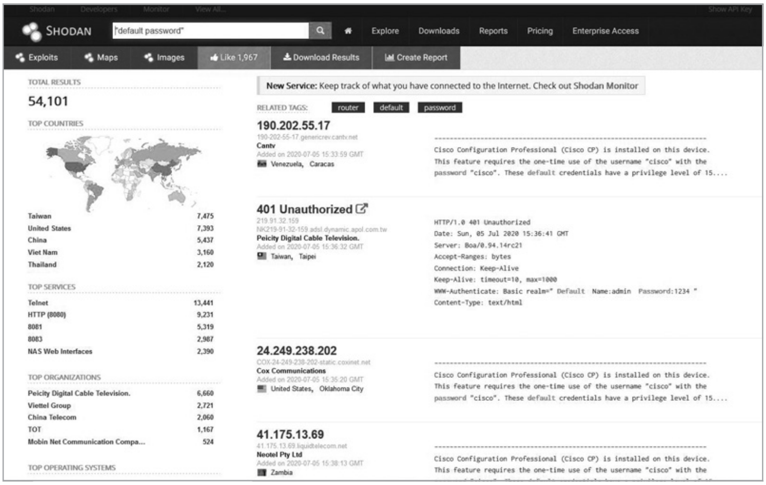
161.35.207.172
Digital Ocean
Added on 2020-07-05 15:09:56 GMT
Germany, Frankfurt am Main
videogame

```
Minecraft Server

Players: 0 online - 10 maximum
Version: 1.16.1 (protocol 736)
Description:
```

Figure 2-6: Minecraft *servers located by Shodan*

Shodan can also provide more serious information, such as information that attackers can use to exploit systems. Return to the Explore page, and this time, instead of selecting Video Games, click **Default Password**, which is about halfway down the page in a light gray box. A list of systems Shodan has verified that use default passwords for their authentication credentials appears, as shown in Figure 2-7.



TOTAL RESULTS

54,101

TOP COUNTRIES

Taiwan	7,475
United States	7,393
China	5,437
Viet Nam	3,160
Thailand	2,120

TOP SERVICES

Telnet	13,441
HTTP (8080)	9,231
8081	5,319
8083	2,987
NAS Web Interfaces	2,390

TOP ORGANIZATIONS

Peicity Digital Cable Television.	6,660
Viettel Group	2,721
China Telecom	2,060
TOT	1,167
Mobin Net Communication Compa...	524

TOP OPERATING SYSTEMS

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

RELATED TAGS: router default password

190.202.55.17
190-202-55-17.genericrev.cantv.net
Cantv
Added on 2020-07-05 15:33:59 GMT
Venezuela, Caracas

```
--------------------------------------------------------------------------
Cisco Configuration Professional (Cisco CP) is installed on this device.
This feature requires the one-time use of the username "cisco" with the
password "cisco". These default credentials have a privilege level of 15....
```

401 Unauthorized
219.91.32.159
NK219-91-32-159.adsl.dynamic.apol.com.tw
Peicity Digital Cable Television.
Added on 2020-07-05 15:36:32 GMT
Taiwan, Taipei

```
HTTP/1.0 401 Unauthorized
Date: Sun, 05 Jul 2020 15:36:41 GMT
Server: Boa/0.94.14rc21
Accept-Ranges: bytes
Connection: Keep-Alive
Keep-Alive: timeout=10, max=1000
WWW-Authenticate: Basic realm=" Default  Name:admin  Password:1234 "
Content-Type: text/html
```

24.249.238.202
COX-24-249-238-202-static.coxinet.net
Cox Communications
Added on 2020-07-05 15:35:20 GMT
United States, Oklahoma City

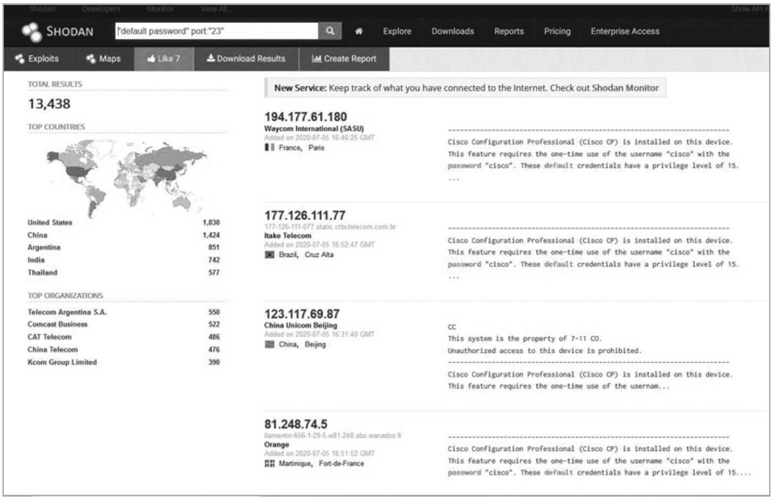
```
--------------------------------------------------------------------------
Cisco Configuration Professional (Cisco CP) is installed on this device.
This feature requires the one-time use of the username "cisco" with the
password "cisco". These default credentials have a privilege level of 15....
```

41.175.13.69
41.175.13.69.liquidtelecom.net
Neotel Pty Ltd
Added on 2020-07-05 15:38:13 GMT
Zambia

```
--------------------------------------------------------------------------
Cisco Configuration Professional (Cisco CP) is installed on this device.
This feature requires the one-time use of the username "cisco" with the
```

Figure 2-7: A list of systems using default passwords

Using a default password is a good way to invite a black hat into your system. Shodan allows you to check whether any of the IP addresses you're using have default credentials. It can also tell you which services you're leaving open to the internet. For example, on the left side, you'll see a list called Top Services. Click **Telnet** to pull up a list of systems that allow Telnet connections, as shown in Figure 2-8.



New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

TOTAL RESULTS

13,438

TOP COUNTRIES

United States	1,830
China	1,424
Argentina	851
India	742
Thailand	577

TOP ORGANIZATIONS

Telecom Argentina S.A.	550
Comcast Business	522
CAT Telecom	486
China Telecom	476
Kcom Group Limited	390

194.177.61.180
Waycom International (SASU)
Added on 2020-07-05 16:46:25 GMT
France, Paris

```
------------------------------------------------------------------------
Cisco Configuration Professional (Cisco CP) is installed on this device.
This feature requires the one-time use of the username "cisco" with the
password "cisco". These default credentials have a privilege level of 15.
...
```

177.126.111.77
177-126-111-077.static.ctbctelecom.com.br
Itake Telecom
Added on 2020-07-05 16:52:47 GMT
Brazil, Cruz Alta

```
------------------------------------------------------------------------
Cisco Configuration Professional (Cisco CP) is installed on this device.
This feature requires the one-time use of the username "cisco" with the
password "cisco". These default credentials have a privilege level of 15.
...
```

123.117.69.87
China Unicom Beijing
Added on 2020-07-05 16:31:40 GMT
China, Beijing

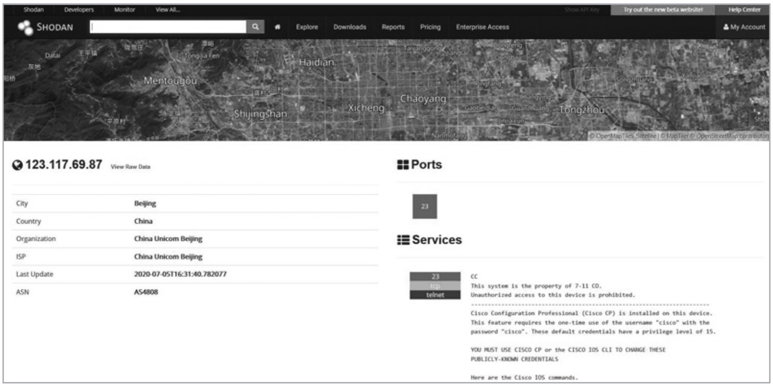
```
CC
This system is the property of 7-11 CO.
Unauthorized access to this device is prohibited.
------------------------------------------------------------------------
Cisco Configuration Professional (Cisco CP) is installed on this device.
This feature requires the one-time use of the usernam...
```

81.248.74.5
lamentin-656-1-29-5.w81-248.abo.wanadoo.fr
Orange
Added on 2020-07-05 16:51:52 GMT
Martinique, Fort-de-France

```
------------------------------------------------------------------------
Cisco Configuration Professional (Cisco CP) is installed on this device.
This feature requires the one-time use of the username "cisco" with the
password "cisco". These default credentials have a privilege level of 15....
```

Figure 2-8: Systems with Telnet open

Telnet allows you to make a remote connection to a system and send it commands as if you were an administrator. It essentially lets you to control the system. Oh, and all Telnet traffic is sent unencrypted. This makes it rather dangerous. But as you can see, a ton of devices allow Telnet connections. Click the IP address in the list to see where these devices are located and other information about them. Figure 2-9 shows an example of a system in China with Telnet open.



123.117.69.87

City	Beijing
Country	China
Organization	China Unicom Beijing
ISP	China Unicom Beijing
Last Update	2020-07-05T16:31:40.782077
ASN	AS4808

```
CC
This system is the property of 7-11 CO.
Unauthorized access to this device is prohibited.
------------------------------------------------------------------------
Cisco Configuration Professional (Cisco CP) is installed on this device.
This feature requires the one-time use of the username "cisco" with the
password "cisco". These default credentials have a privilege level of 15.

YOU MUST USE CISCO CP or the CISCO IOS CLI TO CHANGE THESE
PUBLICLY-KNOWN CREDENTIALS

Here are the Cisco IOS commands.
```

Figure 2-9: An IP record on Shodan for a system in China

Getting paranoid yet? Shodan gives you a massive amount of information about what the public can see about a network on the internet. You can also use it to search for specific addresses. In the search bar, try plugging in the intermediary addresses you discovered during your `tracert` trial to see what comes up. You might not like the results, but at least now you know what your network is putting out for black hats to see.

The key to hiding from an attacker is first knowing what they can see. Using the command line tools in this exercise and Shodan, you can gather that data. If you find that one of your devices is exposed on Shodan, you can take a few steps to close the exposure. First, you'll need to identify which device is exposed. Shodan provides additional details about the connection that can be helpful to accomplish this. Second, you'll need to control the exposure. You have some options here. You can remove the device from the network entirely, although this often isn't viable, because it might not continue to function. You can also look up the manufacturer and find out whether it has recommendations for securing the device. If that doesn't work, forums like Reddit and Spiceworks often provide advice on how to secure home networks. Once you know which device is open, it becomes that much easier to close it.

Conclusion

The internet is a complicated construction of devices and connections that span the globe. Although this can be difficult to conceptualize, you don't need to understand every aspect of the internet to use it securely. By understanding how black hats find targets and how they create attacks against those targets, you can better defend your system when using the internet. The first step is knowing what information you're making public. Once you know what is exposed to attackers on the internet, you can better deploy your own defenses.

3

PHISHING TACTICS

Although it might not seem like it, humans are fairly predictable when it comes to certain behaviors. Black hat hackers know this and use it to their advantage using a technique called *social engineering*, which involves manipulating a person into doing something or revealing some hidden information the victim would normally not do or divulge.

Attackers use social engineering techniques to gain access to your system or data by tricking you. In this chapter, we'll discuss some social engineering techniques that attackers use to gain access to intel, including phishing, URL hijacking, and even hoaxes. By the end of this chapter, you'll have a good idea of how to spot fake messages and counterfeit websites, helping you to avoid any adversaries trying to steal your personal information.

What Is Phishing?

Phishing is one of the most common types of social engineering attacks. It's an attempt to trick a victim into revealing critical information, usually via email. Most likely, you've seen emails that start with an offer to send you a million dollars or promise a cool prize if you just click this link. You might have laughed at the terrible use of grammar or the hilarious premise as you pressed the DELETE key. These are examples of common phishing attempts.

Black hat hackers will try to appear as legitimate individuals or organizations and offer some sort of reward or present a crisis only you can solve. For example, they might pretend to be from your bank and tell you that "You need to respond with your account details before your account is locked out." By adding urgency and intimidation, they're hoping you'll be scared enough to do what they want without second-guessing their tactic.

These attempts usually look for details such as personally identifiable information (PII), credit card numbers, or passwords for important online accounts like your bank or email account. Sometimes they ask for this information directly in the email. Often, they'll ask you to click a link to a website that mimics a real website but is actually a malicious site that will steal and record any information you enter into it, such as your password and username. This is a slight variation of phishing known as *pharming*. We'll talk more about this in "How Black Hats Trick You with URLs."

An Obvious Phish

Sometimes phishing emails are easy to spot and are automatically filtered by your email's spam settings. Let's look at an example of a typical phishing email you might find in your spam folder on any given day:

> Dear Human Greg,
>
> Itz come to our attentionz that you credit card is not update in our database. We has new system that require you to put your infomationz in again. You see, Don spilled a big cup of coffee on the last systemz. I tellz Don, NO YOUZ CANT HAZ COFFEE IN SYSTEM PLACE but he sayz I HAZ COFFEE WHEREVERS. Please, I can haz credit card number? K THX BAI
>
> Sincerely,
>
> Janice, a realz human. (NOT CAT)

This email obviously wasn't sent by an actual person named Janice. It has numerous grammatical errors and includes unprofessional language. It also doesn't mention what service they represent, let alone why they would send you an email directly to update your information rather than having you log into a personal account (which is the typical practice). Additionally, many details are included that would be unnecessary for an account update email. Often, phishing emails will include a narrative intended to get you to trust or empathize with the sender, such as a story about being deported from their country or having recently lost a loved one. The details are provided to confuse or trick you.

Not All Phishing Is Obvious

Not all phishing emails are easy to identify. Let's say you received this email from *customerservice@amazon.org*.

> Dear valued customer,
>
> Your account at <insert your email address> was recently flagged for suspicious activity. Because of this activity, we've temporarily suspended your account and will be permanently deleting it in ten days if you do not verify your information.
>
> To verify your account, please click the link: <malicious link here>. This is an automated message. Please send all replies to accounts@sparklekitten.net.
>
> Sincerely,
>
> Customer Service

This phishing attempt is much trickier to spot. The phisher made sure to write a short, coherent message. It gets to the point—your account is suspended and might be deleted—and uses the social engineering principle of urgency to get you to click a link that will surely take you to some sort of malicious website or even download malware. Frequently, black hats will steal a real company logo to make their emails look more authentic. The preceding example email might have the Amazon or PayPal logo pasted at the top so you assume the email came from one of those companies.

The only real indication that this is a phishing attempt is the email address, *customerservice@amazon.org*. Often, when a phishing attempt is received, it will come from an address that is close to but not quite what the actual company might use. Usually, it contains added words or misspellings, such as *accounts@amzon.com*. If you're unsure about an email, you can always compare the address to other emails you've received from that company to see whether the domains are the same (the domain is the text that comes after the @ symbol).

Using Details for a More Convincing Phish

Sometimes an attacker will target a specific person or organization to gain access to particular data they're trying to steal, so they'll use a technique known as *spear phishing*. Spear phishing uses real information about a person to create an email that looks so authentic it might fool even the best white hat hackers. Let's look at an example:

> Good morning Karen!
>
> This is Steve from the IT Helpdesk. How's everything in HR today? We are supposed to run updates later tonight on your system but I need to make a few changes from your account before I can do that. Can you send me your account login? I'm really swamped down here and don't have time to walk three floors to your office so I was hoping to remote in real quick. Thanks!
>
> Steve
>
> ABC Company
>
> 123 Street
>
> Anywhere, USA

The black hat really did their research for this one. They not only found someone to target who works in HR, Karen, but also found an IT Helpdesk person to impersonate, Steve. By adding little details, like the fact that HR is three floors away from IT, the attacker is able to create trust and familiarity with Karen, which are two more powerful social engineering principles.

Vishing and Other Non-Email Phishing

Email isn't the only way adversaries try to target victims. Phishing can come through any media that allows for communication between people. Instances of phishing attempts have been found in chat apps like Discord, on social media platforms like Instagram and Twitter, and even in games like *League of Legends* or *Fortnite*.

They can also use your phone. A phishing attempt using a phone call is known as *vishing* and can be especially dangerous because the person can react to you in real time. If you sound skeptical or uninterested, the black hat can change their tactics to try to entice you to give them what they want. Frequently, vishing attempts will also impersonate sources of authority, such as the police or the IRS. Imitating authority is a social engineering principle. People have a tendency to immediately trust known authority figures, like a doctor, so it's often advantageous for the attacker to assume such as role.

How to Protect Yourself Against Phishing

It might be easy for you to spot phishing emails now that you know what to look for, but not everyone understands how to spot these attacks. Think about an older relative or loved one, like a grandparent, who might not know the telltale signs of black hat phishing. It's important to help them recognize when an adversary is attacking them, by keeping these common characteristics of phishing emails in mind:

- Phishing emails usually have some sense of urgency or authority involved. If the email says you need to do something immediately or there will be trouble, there's a good chance it's a phish.
- Be sure to check for misspellings, incorrect company logos, or weird email addresses.
- If you've never used a service, it's highly unlikely they'll email you out of the blue. You're not going to get money from a bank at which you don't have an account.
- Tech support will never call you first.
- Always go to the website rather than clicking a link in an email unless you're absolutely sure you know where the email came from.

Teaching your friends and family to consider these details when using email can help them stay safe. You can also create custom rules in their spam filters that will help guard them from common types of phishing. For example, if you know they only use Facebook, you might create a rule that sends any emails from other social media platforms to the spam folder. This will help reduce the amount of phishing emails they have to deal with, making it easier to catch the ones that get through.

How Black Hats Trick You with URLs

Many phishing emails don't just ask you straightforwardly for your information; instead, they'll tell you to click a URL that directs you to a malicious web page where a black hat hacker can harvest your passwords or even install malware on your computer. When you, the victim, click the link, you'll think you're being directed to a perfectly safe web page, so you're likely to enter your important information without a second thought.

A URL, or uniform resource locator, is an address used to find a website, such as *https://www.google.com/* or *https://www.instagram.com.* When you enter that address into your browser, your computer reads it and sends out a Domain Name System (DNS) query, which looks for the IP address associated with that URL. It's similar to your school finding your home address by looking up your name in the school database. Essentially, this is what the DNS does for your web browser: it uses the name (URL) of the website to look up its address (IP address) so the browser can deliver the right web page to you. The DNS is held on a server, either on your local network or in many cases run by your (ISP).

Typosquatting

We use URLs so much that most people don't even pay attention to the web address anymore. That's exactly what attackers are hoping for. Black hats can create their own URLs and use those instead of legitimate URLs to get you to go to malicious web pages. This is known as pharming.

Adversaries accomplish pharming by modifying the content in a URL or on a website. When a black hat misspells a URL, it's known as *typosquatting*. For example, an they might register petmart.com instead of petsmart.com. The DNS then looks up the misspelled URL instead of the real one and sends you to the unsafe website. Today, typosquatting is a rare occurrence because many companies register every possible misspelling of their website name to ensure they all go to the same authentic website.

Complex URLs and Redirects

Black hats also create complex URLs that are hard to read. They do this by creating a long path after the initial URL. A path is where a file is found on a website. For example, *sparklekitten.net/kittenpics* would be the path that accesses the kitten pics section of the sparklekitten.net website. Attackers can use this to their advantage by creating long paths that make it difficult to see where the URL is actually going. For instance, you might get an email with a link that looks like this: *www.accounts.com/user/payments/…* with the three dots indicating that the rest of the URL was cut off. Although this might look like a valid website, there could be a more dangerous portion at the end of the path, such as *payments/files/virus.exe*.

Black hats might also use redirects to hide where their URL goes. A *redirect* is a piece of code that, when activated, sends you to another website instead of the original one you clicked. You might see an ad on a web page that shows a cool new browser game called *Cat Attack!* The ad will look authentic, but as soon as you click the ad banner, instead of going to a cool web game, a script embedded in that web page activates and redirects you to *sparklekitten.net/dumbhooman*.

Redirects are a favorite of adversaries because they're difficult to detect before a person activates them. It's also possible to place scripts and even redirects in real, legitimate websites if that valid website isn't secure (more on redirects in "Web Application Attacks" in Chapter 7).

Modifying DNS Records

Another way that attackers like to pharm is by tampering with DNS records. A DNS server uses records to organize and manage all of the websites and their IP addresses. These records are maintained across all the DNS servers on the internet, so if your DNS server doesn't have a record, it sends out a request to another DNS server until it finds what you're looking for.

If the black hat hacker can modify the DNS record, they can tell your web browser to go wherever they want. They do this by breaking into the DNS server and modifying the record there, causing anyone who queries that server to get the malicious record. Fortunately, altering DNS servers is difficult because they're challenging to break into.

Another pharming technique is to add information to your computer's *local host file*. All computers have a local host file on their system. Any DNS record added to the file will be used instead of sending out a query to a DNS server to find one. If an attacker gets access to that file, they can create their own records. As with modifying DNS records on the server, accessing the local host file is difficult to do.

A much easier way for adversaries to attack your system is to change where your DNS queries go. Instead of them going to the correct DNS server, the black hat can make them go to their malicious DNS server. This is either done locally on your computer or, more often, on a router that your data passes through. Because your system accepts the first record it receives, the attacker can redirect all your internet traffic using their deceptive DNS records. If this happens, not only will links be directed to an unsafe site, but even if you enter *www.facebook.com*, you will still be sent to a dangerous site. The creation of a fake DNS server or record is hard to detect and is currently a hot topic among cybersecurity researchers.

Hoaxes

A *hoax* is a made-up story created to spread false information about a particular subject; for example, on the internet, it could be a fake celebrity story or a new miracle health cure. Hoaxes are initiated for a number of different reasons. Sometimes they're crafted simply as a joke, such as a ruse about new features on the latest iPhone model that don't actually exist.

Hoaxes are also created to damage or spread misleading information about a particular target. For example, a black hat hacker might be angry that a certain cat food company is no longer making their cat's favorite crunchy flavor. Using false reports of health code violations, that adversary might invent a hoax that the company's food is poisonous, thus making people hesitant to buy it.

Most hoaxes are spread through social media. A post or article containing the hoax can quickly spread via Facebook or Twitter posts. Sometimes such deceptions use real information to make them seem more legitimate, which is the reason it can be challenging to expose a hoax and disseminate the right information. Without knowing what is true, it's hard to refute the hoax, especially if it comes from someone you trust.

Deceptiveness can be a powerful weapon. With social media, it's easy for hackers to quickly publicize misinformation about a subject. This can have a huge impact, leading to distrust, anger, and confusion as people find it harder to know what is true. As a large-scale example of such dishonesty, we can look at the 2016 United States presidential election. Several false stories and hoaxes were generated about both candidates, which led to lots of misinformation being spread among the public. Any hoax has the potential to cause harm to people, so we need to always be prepared to recognize one when it appears in our social media feeds.

Why Black Hats Love Phishing

Why do black hat hackers love to use phishing techniques, including URL hijacking and hoaxes, to attack people? Keep in mind that attackers are lazy. Phishing is enticing because it's cheap, easy, and fast.

Phishing attacks are inexpensive to run because all you need is an email server to send messages. Plenty of places will let you rent an email server for very little cost. Even better, instead of paying for their own email server, adversaries might take control of someone else's. This way, not only do they get new email addresses to target from the contact lists on the server, but they can also use that system to send email, making it harder to trace the origin of the phishing messages. Even if only one person in a thousand responds, they're still likely to make a profit.

It's also incredibly easy to set up a phishing email campaign. All the attacker needs to do is craft a generic phishing email and schedule it to send at a certain time. Because phishing isn't time-sensitive, they can just wait until someone clicks the link while they move on to other projects. (Techniques like spear phishing add more complexity to the initial email because it requires custom details about the victim.)

Email is a fast medium; once the email schedule is made, hundreds of thousands of phishing emails can be easily sent in a day. This gives attackers the maximum chance of finding a gullible target in a relatively short time. Once someone clicks or replies, the attacker should have everything they need to exploit their victim.

The biggest reason that black hat hackers love phishing is that it works. It's very difficult to defend against phishing because no hardware or software can fully prevent an attack. Even spam filters miss messages. The likelihood that a spam filter will detect spear phishing is also slim. The only consistent defense against phishing is the person who's being attacked.

Think Twice to Avoid Phishing

Although it might seem as though you always need to be looking over your shoulder for phishing attempts, the best way to stay alert is to question whether an email or phone call makes sense. Doing so will help you recognize an attack.

By stopping to think about what an email is asking or a person on the phone is telling you to do, you can easily identify inconsistencies or gaps in their story. Here are a few critical details to keep in mind when you're questioning a potential assault:

- No company, no matter what, will ever ask you for your password. It might ask you to reset your password but will never ask you for it directly.
- No one ever legitimately contacts you out of the blue, especially to give you something.

- If you're told you have to take action *right now*, step back and think about whether you should do it at all.
- Legal matters, especially criminal, are rarely if ever handled over the phone or through email. Also, you should never pay a fine (for example, a tax fee or criminal fine) without first checking, in person if possible, that it's an official charge.

Take an Alternate Route

Even if you take precautions, it can be tough to recognize when someone is trying to scam you, especially if they're deploying spear phishing tactics. But keep in mind that you always have the option to use another route to check whether something is on the up and up. For example, let's say someone claiming to be from your bank calls and says there's a problem with your account. Instead of dealing with it right then, tell them you're busy and will call back later to fix it. Black hat hackers hate when this happens because they know you won't call them back but will instead call the real bank.

You can use this tactic for any phishing method. Instead of clicking a link sent to you in an email, you can go to the website by searching Google or typing in its URL directly. In fact, you should never click a link in an email unless you're absolutely sure where the email came from. You can also use well-known DNS servers to make sure you're accessing the real site. Changing your browser to use DNS server 8.8.8.8 (Google's DNS) or 1.1.1.1 (Cloudflare's secure DNS) is a good way to avoid DNS hijacking.

Listen to Your Spidey Sense

Don't ever forget that *you* are the best line of defense against phishing attempts. If you see something suspicious, listen to your inner voice and do some research to determine whether it's legitimate. It's also up to you to alert other people about it. Checking whether a source is trustworthy takes extra time, but it helps to prevent false claims from running rampant across the internet.

Exercise: Analyzing a Phishing Email

Part of being skilled at cybersecurity isn't just recognizing a threat, it's also understanding how that threat might hurt you or your organization. This is especially true when it comes to phishing emails. Recognizing certain phishing emails can be challenging. But even if you do recognize and delete one, knowing you've found a phish doesn't provide you with insight about the tricks adversaries use. Instead, when you receive an extremely well-crafted phishing email, you can use your knowledge to detect and analyze it.

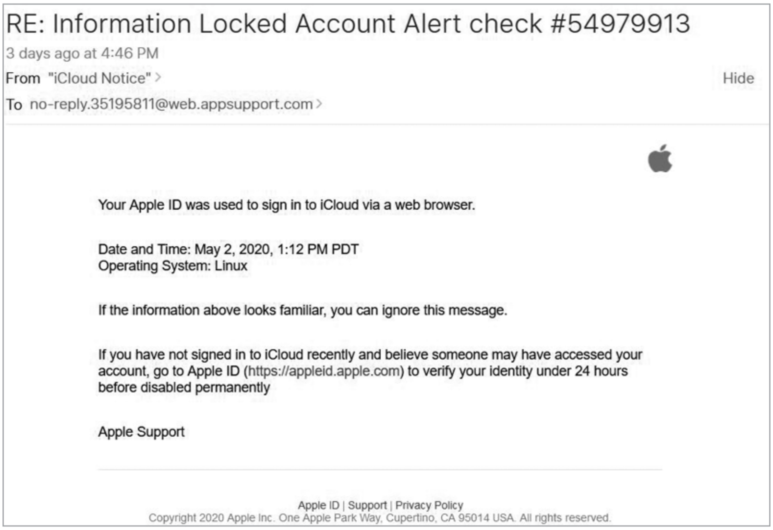
In this exercise, you'll learn how to analyze a phishing email to identify where it came from, whether it's malicious, and what type of attack the black hat was attempting. By the end, you'll know some of the tricks that attackers use to create convincing phishing emails and how to use free online tools to determine whether or not an email is dangerous.

This exercise uses the Gmail platform for its examples. But the information gathered in each step is the same regardless of what type of email application you're using.

WARNING *Analyzing phishing emails can be dangerous.* Under no circumstances should you click a link or open an attachment from a suspected phishing email. *Right-clicking the link will let you* copy the link location *to use for analysis without activating the link.*

Phishing Email Indicators

First, you'll need a phishing email to analyze. Figure 3-1 shows a screenshot of one I received that attempted to impersonate an Apple iCloud login warning. You can usually find a phishing email in your spam folder. Just don't download anything or click any links.



RE: Information Locked Account Alert check #54979913

3 days ago at 4:46 PM

From "iCloud Notice" >

To no-reply.35195811@web.appsupport.com >

Your Apple ID was used to sign in to iCloud via a web browser.

Date and Time: May 2, 2020, 1:12 PM PDT
Operating System: Linux

If the information above looks familiar, you can ignore this message.

If you have not signed in to iCloud recently and believe someone may have accessed your account, go to Apple ID (https://appleid.apple.com) to verify your identity under 24 hours before disabled permanently

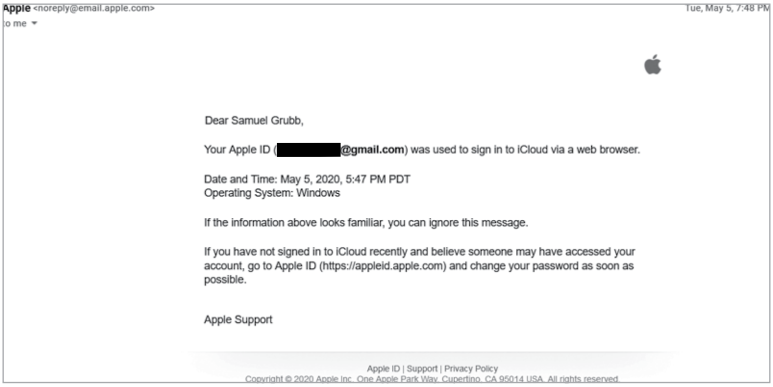
Apple Support

Apple ID | Support | Privacy Policy
Copyright 2020 Apple Inc. One Apple Park Way, Cupertino, CA 95014 USA. All rights reserved.

Figure 3-1: An example of a phishing email

This email purports to be from Apple and claims my account was suspended because of a suspicious login from a Linux operating system. To fix this problem, it says I just need to log in to my account by clicking the link.

This is an incredibly authentic-looking phishing email that closely mimics actual Apple emails. For comparison, Figure 3-2 shows a screenshot of a real Apple iCloud login notice.



Apple <noreply@email.apple.com>
to me
Tue, May 5, 7:48 PM

Dear Samuel Grubb,

Your Apple ID ([redacted]**@gmail.com**) was used to sign in to iCloud via a web browser.

Date and Time: May 5, 2020, 5:47 PM PDT
Operating System: Windows

If the information above looks familiar, you can ignore this message.

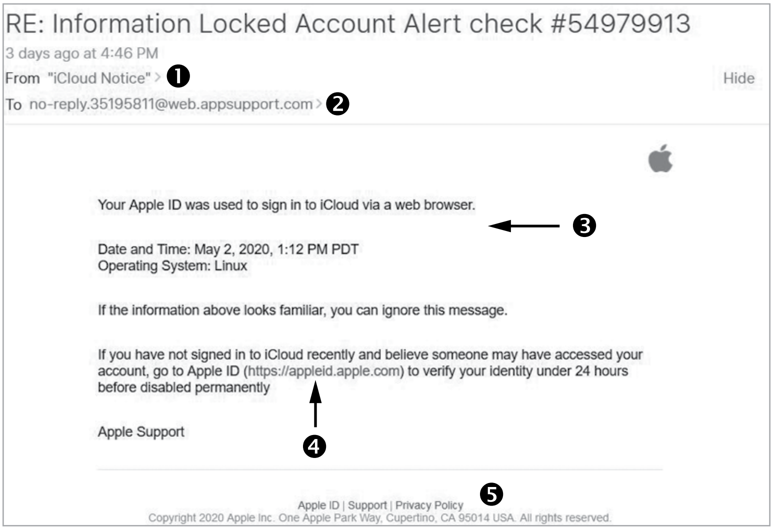
If you have not signed in to iCloud recently and believe someone may have accessed your account, go to Apple ID (https://appleid.apple.com) and change your password as soon as possible.

Apple Support

Apple ID | Support | Privacy Policy
Copyright © 2020 Apple Inc. One Apple Park Way, Cupertino, CA 95014 USA. All rights reserved.

Figure 3-2: A legitimate email from Apple

It looks pretty much the same, right? So, how did I know that Figure 3-1 was a phish? Let's look at it again with a few annotations (Figure 3-3).



RE: Information Locked Account Alert check #54979913
3 days ago at 4:46 PM
From "iCloud Notice" >
To no-reply.35195811@web.appsupport.com >
Hide

Your Apple ID was used to sign in to iCloud via a web browser.

Date and Time: May 2, 2020, 1:12 PM PDT
Operating System: Linux

If the information above looks familiar, you can ignore this message.

If you have not signed in to iCloud recently and believe someone may have accessed your account, go to Apple ID (https://appleid.apple.com) to verify your identity under 24 hours before disabled permanently

Apple Support

Apple ID | Support | Privacy Policy
Copyright 2020 Apple Inc. One Apple Park Way, Cupertino, CA 95014 USA. All rights reserved.

Figure 3-3: The phishing email with numbered annotations

Here is an explanation of these revealing indicators:

1. The email's sender is iCloud Notice, which is suspicious, because you'd probably expect it to just show Apple. Also, it's in quotation marks, which indicates that it's a *friendly name*. Email applications use friendly names as shorthand for email addresses. For example, if your friend Jane has the email address *sparklekittenisamazingdazzle@emaildomain.com*, the application might replace it with the name *Jane* to help you recognize the sender. Later in this exercise you'll see how black hats use this feature all the time to attempt to trick people.

2. The "To" field doesn't include my email address. This indicates that the email was sent using BCC, which hides who the email was sent to. Adversaries use this trick to send phishing emails to multiple victims without tipping them off.
3. The body doesn't contain my account name anywhere. If this alert is supposedly addressed to me, shouldn't my account name be listed? Also, there are numerous grammatical errors throughout the email, including in the last sentence. And the email tries to scare me by claiming my account will be disabled.
4. The link provided is the same as in the legitimate Apple notice, but in this email, it's *active* (clickable). More importantly, when I hover over the link it shows that the URL is something other than what is written, so it's not actually a link to Apple's website.
5. At the bottom of the email are three "links" for Apple ID, Support, and the Privacy Policy. This is probably the hardest indicator to notice. However, when I hover over them, my mouse doesn't give me the telltale hand icon indicating they're clickable links. The reason is that they aren't links at all, but just an image to mimic the signature from the legitimate email.

As you can see, even if the email is very well crafted, there are still several hints that make it apparent it's a phish. But identifying an email as a phish is only the first step of good analysis. The next part is to learn as much as we can about the email by analyzing the header and URL.

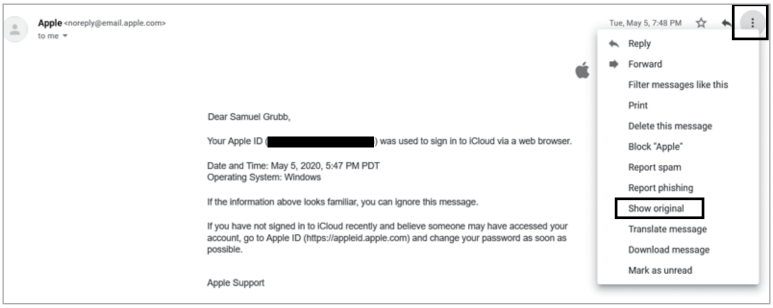
Why is analyzing phishing emails important? Let's say you're working in IT for Sparkle Kitten Inc., and a user calls in saying they received an email but are unsure whether it's legitimate. You might look at the email, realize it's spam, and tell the user to delete it. That's not a bad plan, but what if other users received the same email? What if one of them clicked the link? By taking time to analyze who sent the email and what the URL does when clicked, you'll have valuable information to pass on to your email administrator or security person should this become a problem.

Header Analysis

You'll need to analyze the header first, so you can detect where the email came from and determine any other useful information about it. The email header provides details about the email's origins (as in the stops it took to get to your inbox), who sent it, and other specific information that is included for email servers to read and use.

The process for finding the full email header differs depending on the email application you're using. In Gmail, click the three dots in the top-right corner of the email to access the menu, as shown in Figure 3-4.

In this menu, click **Show original**, as highlighted in Figure 3-4. Doing so will open the email in a new window and provide the full headers in a box below the original To-and From fields, as shown in Figure 3-5.


Apple <noreply@email.apple.com>
to me

Tue, May 5, 7:48 PM

Dear Samuel Grubb,

Your Apple ID ([redacted]) was used to sign in to iCloud via a web browser.

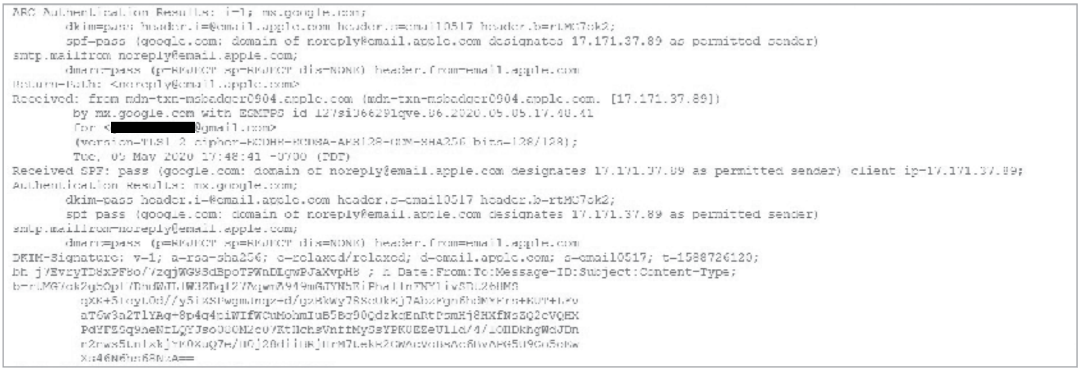
Date and Time: May 5, 2020, 5:47 PM PDT
Operating System: Windows

If the information above looks familiar, you can ignore this message.

If you have not signed in to iCloud recently and believe someone may have accessed your account, go to Apple ID (https://appleid.apple.com) and change your password as soon as possible.

Apple Support

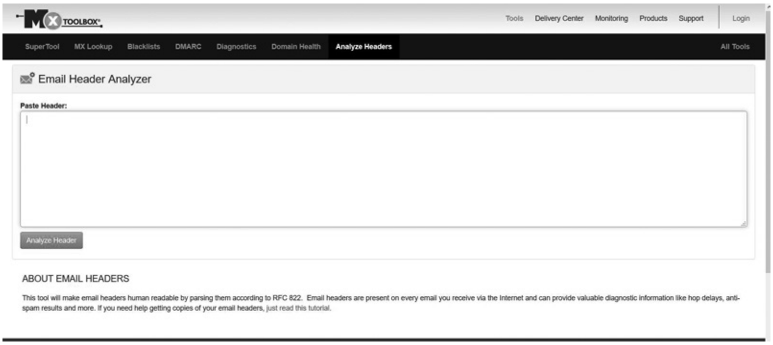
Figure 3-4: The email menu in Gmail



```
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@email.apple.com header.s=email0517 header.b=rtMU7ok2;
       spf=pass (google.com: domain of noreply@email.apple.com designates 17.171.37.89 as permitted sender)
smtp.mailfrom noreply@email.apple.com;
       dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=email.apple.com
Return-Path: <noreply@email.apple.com>
Received: from mdn-txn-msbadger0904.apple.com (mdn-txn-msbadger0904.apple.com. [17.171.37.89])
        by mx.google.com with ESMTPS id 127si366291qve.86.2020.05.05.17.48.41
        for <[redacted]@gmail.com>
        (version=TLS1_2 cipher=ECDHE-ECDSA-AES128-GCM-SHA256 bits=128/128);
        Tue, 05 May 2020 17:48:41 -0700 (PDT)
Received SPF: pass (google.com: domain of noreply@email.apple.com designates 17.171.37.89 as permitted sender) client ip=17.171.37.89;
Authentication Results: mx.google.com;
       dkim=pass header.i=@email.apple.com header.s=email0517 header.b=rtMU7ok2;
       spf pass (google.com: domain of noreply@email.apple.com designates 17.171.37.89 as permitted sender)
smtp.mailfrom=noreply@email.apple.com;
       dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=email.apple.com
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=email.apple.com; s=email0517; t=1588726120;
bh j7EvryTD8xPF8o/7zqjWG93dBpoTPWnDLgwPJaXvpH8 ; h Date:From:To:Message-ID:Subject:Content-Type;
b=rLMG7ok2gbOp[illegible]
        gXK+5[illegible]
        aT6w3a2TlYAq-8p4q4piWIfWCuMohmIuB5Bq90QdzkqEnRtPsmHj8HXfNsEQ2cVQEX
        PdYFZSq9neNrLQYJso0S0M2c07KtHchsVnftMySsYPK0EZeU11d/4/1OHDkhgWdJDn
        n2nws5t[illegible]
        X[illegible]A==
```

Figure 3-5: Email header in Gmail

This plethora of raw data can be hard to read and understand, especially given the number of fields it contains. How do you make sense of such complicated text? You use a tool designed to read the data, of course! The first tool you'll use in your analysis is MX Toolbox. You'll find it free online at *https://mxtoolbox.com/*. MX Toolbox offers a variety of tools to use in email analysis. For now, we'll use the Analyze Headers tool. You'll see it as one of the options on the website's home page (Figure 3-6).



Email Header Analyzer

Paste Header:

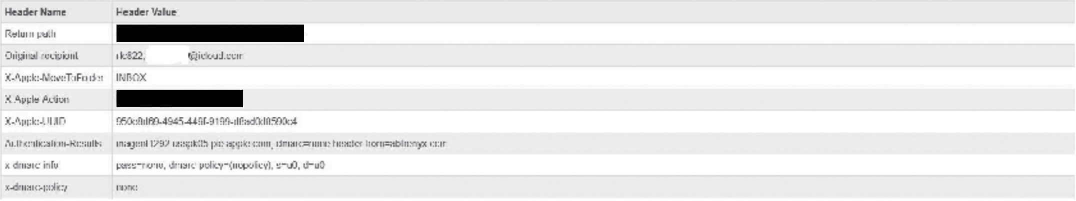
Analyze Header

ABOUT EMAIL HEADERS

This tool will make email headers human readable by parsing them according to RFC 822. Email headers are present on every email you receive via the Internet and can provide valuable diagnostic information like hop delays, anti-spam results and more. If you need help getting copies of your email headers, just read this tutorial.

Figure 3-6: MX Toolbox Analyze Headers tool

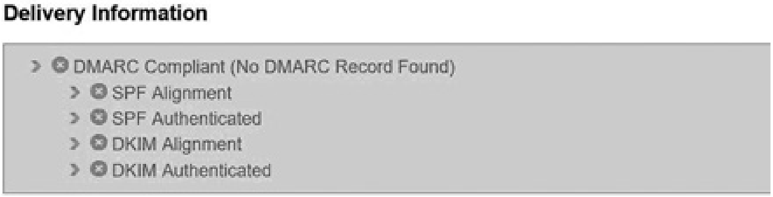
To use the Analyze Headers tool, just copy and paste the full header into the blank window. The tool analyzes the header and separates all the data into easy-to-read fields, as shown in Figure 3-7.



Header Name	Header Value
Return path	[redacted]
Original recipient	rk822, @icloud.com
X-Apple-MoveToFolder	INBOX
X Apple Action	[redacted]
X-Apple-UUID	950c8d60-4945-449f-9199-d6ad0d0590c4
Authentication-Results	imagent 1292 ueqpk05 pic apple com; dmarc=none header from=abtrenyx.com
x dmarc info	pass=none, dmarc policy=(nopolicy), s=u0, d=u0
x-dmarc-policy	none

Figure 3-7: MX Toolbox email header analysis

Before we look at the header fields, we need to examine the findings that appear below the `x-dmarc-info`-Info heading. These are related to two types of authentication that emails use: Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKIM) records, which, together, are known as Domain Message Authentication Reporting (DMARC). Email applications essentially use SPF and DKIM records to verify that the email had permission to be sent from that domain and IP address. For example, if Google sends you an email, it comes from a Google email server with a specific IP address. The address corresponds to a DKIM and SPF record. Your email server checks the DKIM record for Google when it receives the email. If a black hat tries to impersonate Google when sending an email, your server will find that the IP address the attacker is using isn't the same as the one registered to Google. Therefore, the DKIM record will display as failed in the header, as shown in Figure 3-8.



Delivery Information

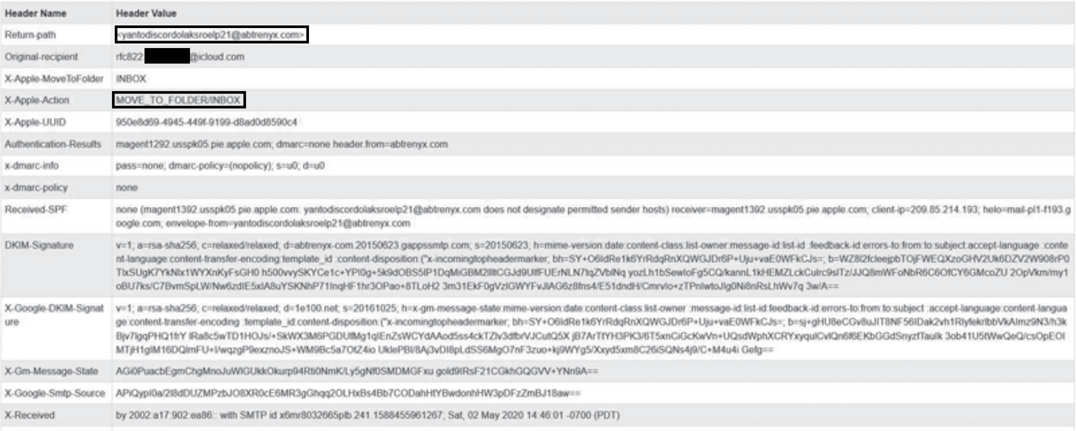
- DMARC Compliant (No DMARC Record Found)
  - SPF Alignment
  - SPF Authenticated
  - DKIM Alignment
  - DKIM Authenticated

Figure 3-8: DMARC failure

Although failed SPF or DKIM records are great indicators of phishing emails, they're not proof. The email server needs to have both DMARC records set up correctly for the signature system to work, and many don't. It's also possible to impersonate an IP to pass a DMARC check, so the fact that an email passes the check doesn't mean it's an authentic email.

Now let's look at the header fields. In Figure 3-9, notice that the address in the `Return-path` field at the top is `yantodiscordolaksroelp21@abtrenyx.com`, which isn't even close to one Apple would use. This address indicates that we're looking at a phishing email. Also, it's best to note the address so an email administrator can look it up later to see whether other users received the email.

Moving down the list of headers, notice the headers that begin with `X`. The `X` headers hold information that the email server reads to decide how to send the email. For example, the `X-Apple-Action` header reads `MOVE_TO_FOLDER/INBOX`. This means that when the email comes into my Gmail account, it's automatically sent to my inbox instead of to junk or spam. Below these headers, you see information about DMARC. As you can see, there is no DMARC policy, which is why the email failed its DMARC check.



Header Name	Header Value
Return-path	<yantodiscordolaksroelp21@abtrenyx.com>
Original-recipient	rfc822;[redacted]@icloud.com
X-Apple-MoveToFolder	INBOX
X-Apple-Action	MOVE_TO_FOLDER/INBOX
X-Apple-UUID	950e8d69-4945-449f-9199-d8ad0d8590c4
Authentication-Results	magent1292.usspk05.pie.apple.com; dmarc=none header.from=abtrenyx.com
x-dmarc-info	pass=none; dmarc-policy=(nopolicy); s=u0; d=u0
x-dmarc-policy	none
Received-SPF	none (magent1392.usspk05.pie.apple.com: yantodiscordolaksroelp21@abtrenyx.com does not designate permitted sender hosts) receiver=magent1392.usspk05.pie.apple.com; client-ip=209.85.214.193; helo=mail-pl1-f193.google.com; envelope-from=yantodiscordolaksroelp21@abtrenyx.com
DKIM-Signature	v=1; a=rsa-sha256; c=relaxed/relaxed; d=abtrenyx-com.20150623.gappssmtp.com; s=20150623; h=mime-version:date:content-class:list-owner:message-id:list-id :feedback-id:errors-to:from:to:subject:accept-language :content-language:content-transfer-encoding:template_id :content-disposition:("x-incomingtopheadermarker; bh=SY+O6IdRe1k6YrRdqRnXQWGJDr6P+Uju+vaE0WFkCJs=; b=WZ8I2fcleejpbTOjFWEQXzoGHV2Uk6DZV2W908rP0 TlxSUgK7YkNlx1WYXnKyFsGH0 h500wvySKYCe1c+YPl0g+5k9dOBS5IP1DqMiGBM2IlltCGJd9UlfFUErNLN7lqZVblNq yozLh1bSewloFg5CQ/kannL1kHEMZLckCulrc9sITz/JJQ8mWFoNbR6C6OfCY6GMcoZU 2OpVkm/my1oBU7ks/C7BvmSpLW/Nw6zdIE5xlA8uYSKNhP71lnqHF1hr3OPao+8TLoH2 3m31EkF0gVzIGWYFvJlAG6z8fns4/E51dndH/Cmrvlo+zTPnlwtoJlg0Ni8nRsLhWv7q 3w/A==
X-Google-DKIM-Signature	v=1; a=rsa-sha256; c=relaxed/relaxed; d=1e100.net; s=20161025; h=x-gm-message-state:mime-version:date:content-class:list-owner :message-id:list-id:feedback-id:errors-to:from:to:subject :accept-language:content-language:content-transfer-encoding :template_id:content-disposition:("x-incomingtopheadermarker; bh=SY+O6IdRe1k6YrRdqRnXQWGJDr6P+Uju+vaE0WFkCJs=; b=sj+gHU8eCGv8uJIT8NF56IDak2vh1RIyfekrIbbVkAImz9N3/h3kBjv7lgqPHQ1frY lRa8c5wTD1HOJs/+SkWX3M6PGDUfMg1qIEnZsWCYdAAod5ss4ckTZlv3dfbrVJCutQ5X jB7ArTfYH3PK3/6T5xnCiGcKwVn+UQsdWphXCRYxyqulCvlQn6f6EKbGGdSnyzfTaulk 3ob41U5tWwQeQ/csOpEOlMTjH1gIM16DQlmFU+l/wqzgP9exznoJS+WM9Bc5a7OtZ4io UkIePBI/8Aj3vDI8pLdSS6MgO7nF3zuo+kj9WYg5/Xxyd5xm8C26iSQNs4j9/C+M4u4i Gefg==
X-Gm-Message-State	AGi0PuacbEgmChgMnoJuWIGUkkOkurp94Rti0NmK/Ly5gNf0SMDMGFxu gold9IRsF21CGkhGQGVV+YNn9A==
X-Google-Smtp-Source	APiQypl0a/2I8dDUZMPzbJO8XR0cE6MR3gGhqq2OLHxBs4Bb7CODahHtYBwdonhHW3pDFzZmBJ18aw==
X-Received	by 2002:a17:902:ea86:: with SMTP id x6mr8032665plb.241.1588455961267; Sat, 02 May 2020 14:46:01 -0700 (PDT)

Figure 3-9: Header with highlighted fields

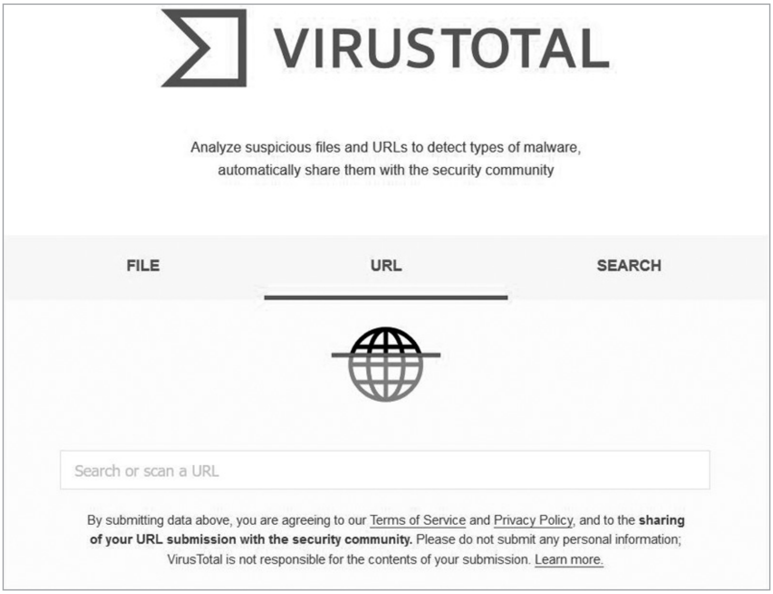
Table 3-1 lists some other headers to look for and the information you can gather from them.

Table 3-1: Important Email Header Fields

Field	Purpose
`Message-ID`	Unique ID given to the email. Makes it easy to find using search functions.
`x-originating-ip`	Original IP address that sent the email. Helps determine whether or not the sender was known as malicious, as well as find other messages sent by that sender.
`X-Mailer`	Specifies the application used to send the email. Weird or unexpected platforms might indicate a phish.
`Received-SPF`	Provides results of SPF check.
`X-MS-Has-Attach`	Indicates whether or not the email had an attachment.

URL Analysis

After looking at the headers, you need to verify whether the URL is malicious. To do this, you'll use another online tool called VirusTotal, which is available at *https://www.virustotal.com/gui/home/url/*. Figure 3-10 shows its home page.



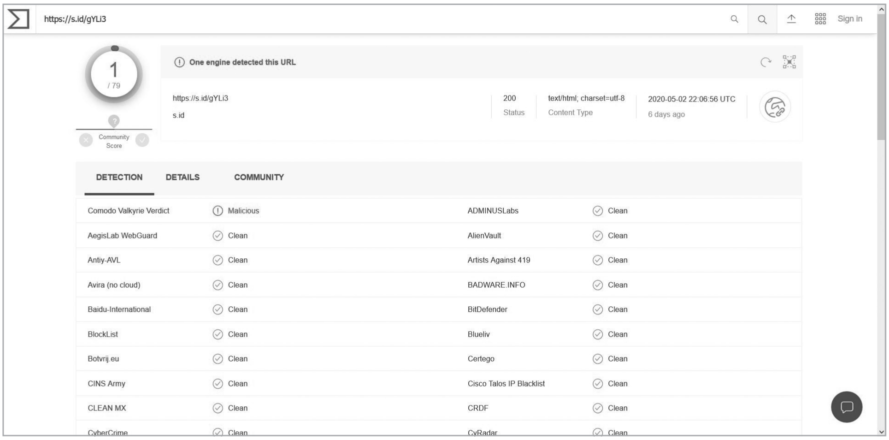
VIRUSTOTAL

Analyze suspicious files and URLs to detect types of malware,
automatically share them with the security community

By submitting data above, you are agreeing to our Terms of Service and Privacy Policy, and to the **sharing of your URL submission with the security community.** Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.

Figure 3-10: The VirusTotal home page

VirusTotal allows you to scan URL links for malicious behavior by using a multitude of antivirus engines, which we'll discuss in more detail in Chapter 4. It runs the link through each engine and aggregates the information on a page that's easy to understand and share. If even one engine flags it as malicious, you should assume the link is malicious. Figure 3-11 shows the results of running the link in Figure 3-2 through VirusTotal.



https://s.id/gYLi3

One engine detected this URL

https://s.id/gYLi3
s.id

200 Status

text/html; charset=utf-8 Content Type

2020-05-02 22:06:56 UTC
6 days ago

Comodo Valkyrie Verdict	ⓘ Malicious	ADMINUSLabs	✓ Clean
AegisLab WebGuard	✓ Clean	AlienVault	✓ Clean
Antiy-AVL	✓ Clean	Artists Against 419	✓ Clean
Avira (no cloud)	✓ Clean	BADWARE.INFO	✓ Clean
Baidu-International	✓ Clean	BitDefender	✓ Clean
BlockList	✓ Clean	Blueliv	✓ Clean
Botvrij.eu	✓ Clean	Certego	✓ Clean
CINS Army	✓ Clean	Cisco Talos IP Blacklist	✓ Clean
CLEAN MX	✓ Clean	CRDF	✓ Clean
CyberCrime	✓ Clean	CyRadar	✓ Clean

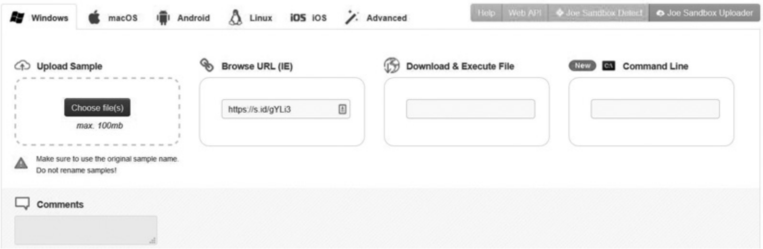
Figure 3-11: Analysis from VirusTotal

Even though only one engine returned positive malicious results, it's enough to know that this link is bad.

Like any good security expert, you have a burning curiosity to know what happens when you click the link. However, you also know that clicking the link could potentially infect your computer. So what do you do?

You use another tool called Joe Sandbox (*https://www.joesandbox.com/*). This is a free tool that lets you run attachments or open URLs in a sandbox environment. *Sandboxes* are simulated computers meant to act like real, physical machines, but you can isolate them from the rest of your computer system and destroy them easily. This makes them perfect for testing malicious entities like malware, because you can study the malware infection without worrying that it will spread or damage critical system components.

To begin using Joe Sandbox, create an account. Then copy and paste a link into the sandbox, as shown in Figure 3-12.



https://s.id/gYLi3

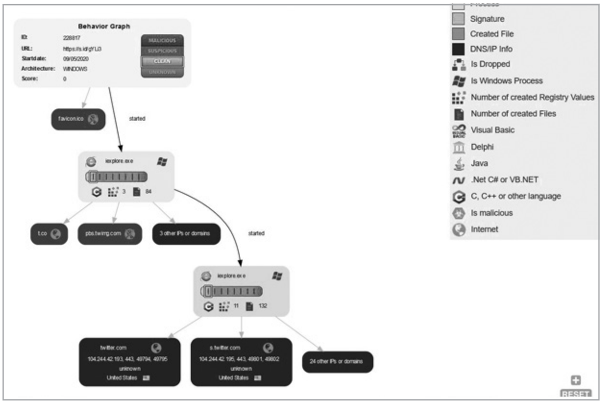
Make sure to use the original sample name.
Do not rename samples!

Figure 3-12: Joe Sandbox's home page

NOTE *Unless you pay for a private account, all results from the sandbox will be made public for other researchers to see. Don't submit anything that might contain personal information.*

It takes a few minutes for the report to generate, but once it does, you'll be provided with a wealth of information about the link and what runs when you click it. The two most interesting features are the Behavior Graph and Screenshots section.

The Behavior Graph (Figure 3-13) shows all the processes that happen when someone clicks the link, such as anything that opens or any web pages that are accessed. In this example, the link opens a few different web pages and then redirects to additional ones. You can tell that none of these are actual Apple domains, which is further proof that this email didn't come from a valid Apple source.

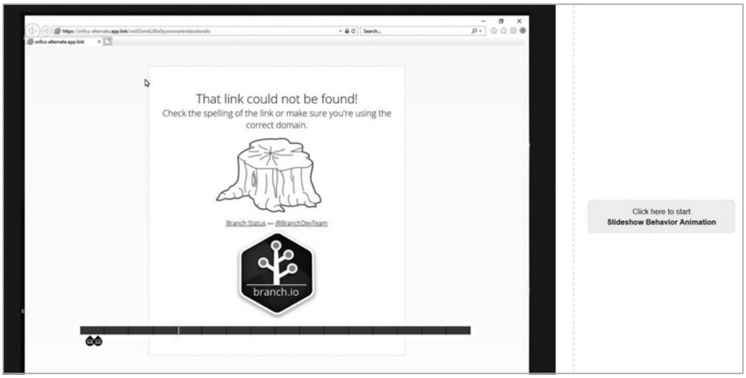


Behavior Graph

ID: 228817
URL: https://s.id/gYLl3
Startdate: 09/05/2020
Architecture: WINDOWS
Score: 0

Figure 3-13: Joe Sandbox report: Behavior Graph

The Screenshots section (Figure 3-14) shows screenshots of what opened or ran when the sandbox executed the link.



That link could not be found!

Check the spelling of the link or make sure you're using the correct domain.

Branch Status — @BranchDevTeam

Figure 3-14: Joe Sandbox report: Screenshots section

This section also has an animation option, so you can watch what happens in real time. The particular link I submitted couldn't be found, which, although unfortunate for our research purposes, isn't surprising. Phishing links typically remain active for only a limited period of time before they're either discovered or removed by the phisher to avoid detection. Still, because the email asked you to verify your account, you now know that this was likely a *credential hijacking* attack. In this type of attack, an adversary attempts to steal credentials, either by having the victim enter them in a fake site or by using browser vulnerabilities to capture them.

With a little research and a few free tools, you can learn a lot about phishing emails. You've now analyzed this email and determined that it's a phish, the source of the attack, and what type of attack was attempted. You can now better protect yourself by adding rules to your email program that instruct the server to send any message from this malicious sender directly to your junk box or to pass this information to the appropriate administrators to use in their defense efforts.

Conclusion

When it comes to phishing, it's critical to remember that it only takes one click for an attacker to gain access to your computer or potentially steal your personal information. Phishing can come from many different directions because basically an attacker can use any form of social engineering communication. Be on the alert every time you use email or receive a phone call. With practice, you'll learn how to recognize phishing attempts more easily. Whether the attack uses pharming, vishing, spear phishing, or any other type of social engineering, take time to think through what is being asked of you. Doing so can be the difference between a successful and unsuccessful phishing attack.