HACKING

Network Protocols

Complete Guide about Hacking, Scripting and Security of Computer Systems and Networks.

Hans Weber

Hacking Network Protocols

Complete Guide about Hacking, Scripting and Security of Computer Systems and Networks.

Hans Weber

This document is geared towards providing exact and reliable information in regards to the topic and issue covered. The publication is sold with the idea that the publisher is not required to render accounting, officially permitted, or otherwise, qualified services. If advice is necessary, legal or professional, a practiced individual in the profession should be ordered.

- From a Declaration of Principles which was accepted and approved equally by a Committee of the American Bar Association and a Committee of Publishers and Associations.

The information provided herein is stated to be truthful and consistent, in that any liability, in terms of inattention or otherwise, by any usage or abuse of any policies, processes, or directions contained within is the solitary and utter responsibility of the recipient reader. Under no circumstances will any legal responsibility or blame be held against the publisher for any reparation, damages, or monetary loss due to the information herein, either directly or indirectly.

The information herein is offered for informational purposes solely, and is universal as so. The presentation of the information is without contract or any type of guarantee assurance.

The trademarks that are used are without any consent, and the publication of the trademark is without permission or backing by the trademark owner. All trademarks and brands within this book are for clarifying purposes only and are the owned by the owners themselves, not affiliated with this document.

Table of Contents

Hacking Network Protocols

BOOK 1 - Computer Systems and Networking Guide: A Complete Guide to the Basic Concepts in Computer Systems Networking, IP Subnetting and Network Security.

INTRODUCTION

CHAPTER ONE: AN INTRODUCTION TO COMPUTER SYSTEMS AND NETWORKING

CHAPTER TWO: INSIDE THE COMPUTER SYSTEMS AND NETWORKING CONCEPT

CHAPTER THREE: COMPUTER SYSTEMS NETWORK AND SECURITY

CHAPTER FOUR: COMPUTER SYSTEM NETWORK: SETTING UP YOUR OWN

CHAPTER FIVE: IP AND SUBNETTING EXPLAINED

CHAPTER SIX: APPLYING THE CONCEPTS OF COMPUTER SYSTEMS NETWORK

CHAPTER SEVEN: OUTSIDE THE NETWORK NUMBERS: WHAT STILL MATTERS

CONCLUSION

BOOK 2 - Hacking: A Quick and Simple Introduction to the Basics of Hacking, Scripting, Cybersecurity, Networking and System Penetration.

INTRODUCTION

CHAPTER 1: BLACK HAT HACKING

CHAPTER 2: WHITE HAT HACKING

CHAPTER 3: GREY HAT HACKING

CHAPTER 4: NETWORKS

CHAPTER 5: SCRIPTING AND OTHER TOOLS

CHAPTER 6: THE DIFFERENT TYPES OF HACKING AND HOW THEY WORK

CHAPTER 7: HOW TO PROTECT YOURSELF FROM HACKING

CHAPTER 8: CYBERSECURITY AND HOW IT SAVES YOU FROM BEING HACKED

CONCLUSION

Computer Systems and Networking Guide

A Complete Guide to the Basic Concepts in Computer Systems Networking, IP Subnetting and Network Security.

Hans Weber

Introduction

How much do you know about a computer today? It’s not just about knowing the basics. Computer networking is what drives in the world today, and if you are looking for a career as a computer networking specialist, now is the time.

Computer system networks are the backbone of most companies set by today standards. Even more so, it’s the backbone of all major companies successful in recent times.

Anyone who can understand its importance and knows how to exploit them can safeguard their ventures from most of yesterday’s issues. They provide a seamless way to keep logs, inventories, transactions, and payrolls; these networks are also the primary communications channels right now.

With this guide, you’ll acquire all the knowledge necessary for a first grasp on the subject. That knowledge will be the main pillar for anyone looking to implement similar networks; anyone looking to study and specialize in computer system networks will also get the best starting point for their journey.

What can you expect to understand after finishing the content inside this book?

First, you’ll know the most basic concepts: how these networks started, what makes them up, and how you can identify one. Through the first chapters, you’ll learn the fundamental knowledge about them.

Naturally, the book will deepen the knowledge as the reader continues.

After understanding the concept, you’ll move into the most intricate concepts necessary to set them up: IPs, subnetting, and even how to establish a good security system for keeping your network safe.

The book covers both how to set up a secure network as well as what dangers you could face when establishing your systems.

Finally, you’ll learn how these systems apply to different industries and company models.

In the end, the reader will know all they need to understand the necessary steps and concepts necessary to integrate and exploit these systems to their fullest.

Chapter One: An Introduction to Computer Systems and Networking

How did it start?

If we are going to start talking about computer systems and networks as a career, we have to understand its history and how it became an in-demand job today.

"Information technology," better known as IT, is defined as the technology that involves the development, use and maintenance of computer systems, software and networks for the distribution and processing of data. The term goes way back to 1978.

Computers did exist before 1978, but they were mostly used to perform calculations. Since they started to be used to index and sort written information, the term IT was invented.

Today, IT is a quickly evolving field and that, of course, includes the computer systems and networking career inside this branch.

Computer systems and networking. What exactly is it?

The IT career is based on the upkeep, configurations and reliable operation of the computer system, especially the process of multi-user computers and its networks with other users.

Nowadays, companies rely on their networks for a lot of their work, so any issues must be fixed quickly and entirely.

The computer systems and network administrator keeps the organization's workflow and its lines of communication accessible - at all times necessary. Besides identifying and solving network problems, computer systems administrators also make updates to all hardware and software they manage, so they're always ongoing.

A computer systems administrator is the main point of contact for an organization's network users when they suffer some technical issues. The specialist also needs to guarantee that every connection in the office is working well and supervise the performance of the Internet optimizing their hardware and software.

A computer system and network administrator also make sure that the overall performance and security of the computers they supervise, fulfil the needs of the network users, without surpassing the company's budget.

The person in charge of this job needs to be ready to find new issues each day and needs to get their knowledge optimized to approach them efficiently.

The importance of the field in the current era

Today, companies look at networks and computer systems as their foundation to work optimally.

They need their hardware to be highly functional and maintainable, they need their Internet and servers stable, and they need someone to do all the networking and cable installation and check-ups constantly around their offices.

As we said before, they are the ones responsible for the configuration, reliable operation and upkeep of computer systems inside the office. They seek to ensure that the uptime, performance, resources and security of the computers they manage to meet the needs of all the users.

Today, companies are very dependent on this type of professionals. They need to check the performance of their systems and need a person available almost 24/7 to guarantee that everything is functioning as it should. If one of their servers are down, or they lose Internet connection, they start to lose money very quickly mainly because they stop their production for a certain amount of time, and there is no way to monetize the operation without it working efficiently with the connections and servers.

A computer system administrator or specialist is one of the most critical professionals inside every office nowadays.

The computer systems and networking administrator is also the one in charge to guarantee that the Internet connection is working correctly and that the mail server is running and processing emails that are being sent and received by all staff within the organization.

If this task isn't well-executed, it might lead to a lot of expensive problems for the company such as serious mistakes in the production and handling of their job to significant money problems and losses. Here is a list focused on why it is essential to have a computer system and network specialist:

A specialist in this field maintains the operating system of the serves and applications, such as mail services, web services and more. They troubleshoot any hardware, OS or application-related problems to ensure the whole operation of the company itself.

A computer system and network administrator is in charge of maintaining the network infrastructure, such as routers and switches and fixing network-related problems. They attend every single detail about the networks and cables going around the office and how to keep them and the security of people working there.

They are also in charge of one of the most critical jobs inside an organization, and that is keeping the database system used by the company. In bigger organizations, this is a highly essential task, to secure all the data and to keep it optimized and safe from third parties, and possibly losses.

This type of specialist is the one that coordinates the daily operation of secure systems. They handle the monitoring systems and the running of regular backups. They set up, delete and manage individual user accounts.

They keep every single system updated and working on its optimal conditions.

An overview of the process to become a computer system network specialist

When wanting to become a computer systems administrator, there is no one single way of learning. Educational requirements commonly include getting a bachelor's degree in computer science, web technology or network administration. Therefore, anyone who wants can become a computer systems administrator by self-learning or on-the-job training.

Some employers may need their administrators on computer systems to hold a certificate or proof of training from some specific software. There are some training methods and certification intended for specific IT fields such as Microsoft training and certification for Microsoft-based systems like Microsoft Windows and SQL. Another certification they might be looking for is a Cisco training certification for Cisco networks.

To become a computer system and network specialist or administrator, the first thing to aim for will be education.

While most employers want their network and computer systems administrators to have a bachelor's degree, others only need a postsecondary certificate.

Many degree programs focus on computer network and system administration. Because administrators work with computer equipment and hardware, a degree in computer engineering or electrical engineering is adequate as well. Programs in this area frequently include classes in networking, computer programming or systems design.

Because this technology is always changing and evolving, administrators need to keep up with all the recent developments.
Many specialists in this field keep taking courses throughout their careers and attend information technology conferences to keep updated with the latest technology as well. Some businesses need that administrators have a master's degree in IT.

Organizations generally want their network and computer systems specialists to be certified in the products they use. Certification programs are usually offered from the vendor or vendor-neutral certification providers. These certifications validate the knowledge and the use of the best methods that are needed of the network computer systems administrators. One of the most standard certifications is the one Microsoft offers.

Network administrators can work and study enough to become computer network architects. They can also advance to managerial jobs in IT departments, like computer and information system managers.

Here is a list of essential qualities everyone who wants to get into this career must have:

- **Analytical Skills**. Every computer systems and network administrator or specialist needs to evaluate networks and policies to ensure that they perform reliably and to prepare to new customer's requirements and changing needs.

- **Multitasking skills**. Every computer systems and network aspirant will have to work on many problems and tasks at the same time.

The ability to deliver an excellent job while multitasking is one of the most important items on this list.

- **Communication skills**. A lot of people overlook this quality when it comes to this career, but its importance relies on the moment when they have to describe the problems and the solutions to non-IT workers.

- **Responsibility**. This is one mind-changing quality everybody should have, but when it comes to a computer system and network specialist, it is crucial. They manage the whole functioning of an entire company and how their production and work is on its optimal condition. Without responsibility, the company can suffer a lot of losses and issues due to lack of conscience from their IT department.

- **Quick Learning**. As we mentioned many times before, the IT world is always changing and evolving and adding new systems to the list. For a computer system and network administrator, it is crucial to be updated with the software and hardware to ensure the best outcome for the organization.

- **Programming skills**. This is a perfect add-on to every computer system specialist, as sometimes you will need to go a little deeper when it comes to working with a particular server or web technology challenge, and the new knowledge will boost your work.

An overview of what makes an excellent specialist profile

What makes the right specialist for a company these days relies on many things, not only education.

It is not a simple profession, but that is what makes it so demanding. The computer system administrator is a crucial figure in any company, and it has always been a high profile when it comes to knowledge and qualities.

A computer system administrator is an essential part of a big or strong organization IT team. The positions do vary from business to business, but they are all responsible for managing the same things and duties.

These IT professionals must work closely with employees to install updates on computers and provide tech support when the problems appear.

Here are some traits that all excellent computer system and networking specialist must fulfil:

Patience. This is a crucial trait of any good systems administrator. Many times, the employees may be unfamiliar with certain computer functions. When it comes to optimizing or making changes, administrators need to have the patience to lead employees through the different challenges.

Especially, when it comes to hardware or software issues, it can take a while for employees to do it the right way. In this case, the user is likely to be angry or irritable because they don't understand what to do with their computer or why it is not working as it should. A good system administrator needs to be able to respond with a patient and understanding manner to help and resolve the problem, to also minimize employee frustration. Patience goes first when we talk about managing computer issues.

Flexibility. If you are doing a significant company-wide software upgrade and suddenly one of your primary servers fails, a competent system specialist will be able to quickly prioritize and be flexible when a potential hardware crisis arises. They need to know which upgrades to focus on first and which to pause given the current circumstances .

A flexible approach here can help understand the priority route to take when it comes to dealing with your company's problems. When looking for a candidate to take a job like this, it is essential to pick a multitasker. You need someone who is up to the challenges.

Technical Knowledge. Arguably the essential trait of any good systems administrator is a comprehensive understanding of computer equipment, hardware and software. You need to have strong technical knowledge to be able to figure out the solutions – especially when things aren't working as they should.

Embedded systems administrators typically have professional experience in an enterprise environment, plus numerous relevant certificates in their field. When hiring or interviewing new candidates, asking them questions related to their technical knowledge will determine how much they know about what they do.

Personable Nature. A computer system and network administrator frequently works with other employees. Operations and network specialist need to know how to communicate clearly and manage difficult personalities while staying calm under pressure and tight deadlines.

How do computer systems and networking improve a company?

When running a growing business, we start to understand that quality IT solutions are crucial to a company efficiency. And computer networks are one of the most critical IT solutions. They help the business grow and let employees share ideas rapidly and work more efficiently. It increases their productivity and creates more income for the company.

Excellent computer systems and network administrators also reduce the amount of money that is spent on hardware by creating a computer network and sharing the equipment you already have.

With a professional on your IT team, you also improve storage efficiency and volume, you have the freedom to choose the best computer networking method for your team to display. Hiring a professional computer systems and network specialist also gives you a lot of flexibility.

Information technology has for a long time dominated the industrial segment. Since the inception of microprocessors, this field hasn’t witnessed a dark stage. Each year, we witness a significant change in this domain that brings the real world closer to the virtual one. Smartphones, smart televisions, gaming consoles, motion-sensing devices are all wonders of the IT field. In fact, IT has become an integral part of our lives and it is difficult to imagine a world without it.

Information Technology and Business – What’s the connection?

Information technology is required by companies to reduce costs, increase efficiency as well as gain dominance over the market. From website hosting and storage of data to strategy formulation and social networking, IT offers a wide array of corporate solutions. Strong integration of IT is done by businesses leaders to accomplish these goals. Nonetheless, there are certain domains under information technology that are trending and expect to grow exponentially in the near future.

Why should you be keeping an eye on these trends?

It is extremely likely that these trends in Information Technology will be the point of focus in the coming years. Basically, these trends refer to those sectors that allow companies to enhance productivity and make their consumers aware about their range of products and services. Businesses from all over the world will be looking to exploit the potential of these technologies.

Here are the top technology trends that according to analysts will be the game changers in the near future.

Private Cloud: The private cloud is an excellent alternative to public cloud computing as it resolves all the security issues posed by the latter. Consumers of information technology demand more from the services it provides. Wouldn’t it be great if a business could reduce the time-to-market and operate in a cost-effective manner? Every company will want this.

As the private cloud is deployed within the company firewall, all the data can be shared among the employees without having to worry about security breaches.

Cyber Security: This continues to be a cause of serious concern among the IT companies all across the globe. It would be dangerous if someone had access to a company’s records and data pertaining to tenders. Our economies, nations, corporations are all interconnected. In fact, most organizations survive on the Internet. Compromising with cyber security can have a devastating impact on the global economy. This has become increasingly essential as Internet-based attacks will increase in the coming years.

Enterprise Social Networking: This is the next big thing in the corporate world. Every company would want to market its new products and enhance brand awareness. As more and more people are getting onto social websites, it has become easy to connect with them on social networks. In the coming years, it is anticipated that people will become more comfortable with using such websites and carry out business transactions over the Internet. Businesses that succeed in becoming social organizations have a better run on the market.

Gamification: This is one of the leading trends in information technology. Companies that focus on enhancing user experience are more successful. Gamification employs gaming mechanics, interactive media and social networking to accomplish this.

Gamification is done to deepen connection with consumers so that they interact well with the company. Gaming has for a long time been a very profitable domain and leading edge companies will also be looking to explore its potential.

Chapter Two: Inside the Computer Systems and Networking Concept

The Computer System

A computer system is the intricate union of physical pieces called hardware, and programs or applications called software. A user, or live ware, uses this machine to find, sort, and manage varied information. It should be able to input data from an external source and process this data. Also, if needed, it should be able to convert this information into a format that can be used externally.

The essential hardware elements that it needs are a monitor, a mouse, a keyboard, and a CPU. Depending on the use that the user intends to give it, it can have a significant number of programs, divided between system software and applications software. The keyboard and mouse are input devices that help to introduce information into the computer and manage that information to give it the format intended.

With a computer system, a user can work with different kinds of information: text, images, sounds, videos, etc. It can transform that information into another format. With that, it creates original projects by mixing the different formats into a final project that can be exported or stored inside the computer or an output device. Examples of output devices are printers, recorded discs, and external hard drives.

Networking and Computer Systems

A computer system network is when two or more computers systems are interconnected, creating a net between them. Through this network, a user can share information with other users without using external output devices. A computer network can be done by physically connecting computers using wires, or through a wireless connection using Bluetooth or WI-FI.

In business, having a computer network is very useful. With all the computers systems linked to each other, supervisors can evaluate their employee's work, and managers can organize the information effectively. It makes it easier to communicate between different departments, to send memos individually or to all the company members at the same time.

Workgroups can coordinate better between them, sending reports daily so they can all know the advances they have made with the project. They can join through the same programs and add their ideas without being in the same physical place. The final project can be sent to the head of the department for their approval.

It is also essential when managing confidential information only known to those who work in the company. It prevents leaks that could put at risk the future of the business, keeping the relevant information to those who manage the keywords and passwords.

IP and Sub Netting

An IP, or Internet Protocol address, is the number that is assigned to a specific computer system inside a network and allows that computer to communicate with others through the Internet. Four numbers divided by dots form it. Each number have between one and three digits that go from 0 from 255.

This address indicates other computers where it is located around the world. Every address is different from the next one, and depending on the specific set of numbers and digits, it can be known as its exact location. Without IP addresses it would be impossible to communicate by email or peruse through the Internet to search for information.

Sub-netting is the action of dividing a network into small sub networks or subnets. It is advantageous when a company wants to add new subnets but doesn't want to get a different network address. At first, the idea of sub-netting was though as a solution for the shortage of IP addresses.

After many years, sub-netting has proved to be essential as a method of reducing network traffic. The networks come in the classes: Class A, B, and C. When sub-netting, the classes are divided into small portions, the subnets. These subnets can also be separated in even smaller codes if needed.

By doing so, the user is allowed to have a work network in the house, without having to get a new one.

Elements inside a Computer System Network

When working with a computer network, it is essential to take many factors into consideration. The correct use of them can make a difference in any business.

- **Computers**: To create a computer system network, you must have at least two computers that will be working together. They don't need to be in the same room, some of them may even be in houses also if it is a company network. This allows the managers to work from their homes instead of moving to an office.

The characteristics of the computer systems don't have to be the same, although it is recommended. That way, you can be sure that all the computers support the programs that you will need to use for your business.

- **IP**: Once you obtain an IP address for your network, you can divide them into subnets, assigning one for each computer of your system. That way, the computers can share information faster and reduce the volume of the broadcast.

Also, when working with a Local Area Network (LAN), it allows it to manage the constraints, such as the maximum number of hosts permitted in the network.

-**Security**: A computer network needs to have a good security system. To have many computers linked and sharing information can seem risky, especially if the computer is not inside a secure room.

The security measures can be both for the hardware and the software.

You must install passwords and codes hard to crack by an outsider. You should also install security programs that can protect your information from the inside, with firewalls and virus detectors .

Many safe security systems can be downloaded for free or paid. You can also hire an expert programmer that can build a security system customized to your needs.

-Employees: The use that your employees will give to the computer system network is also important. Depending on the kind of business that you manage, your employees will spend more or less hours in front of the computer.

One of the essential rules that those who work for you must know is that the computer system is not for personal research and use. It is a company asset, so employees are responsible for their behavior. Improper use of the computer can develop into the reduction of the useful life of the asset.

The employees must get familiar with the programs they will be using and follow the correct instructions. Managers will be able to evaluate their jobs from their computers, keeping organized work.

Computer System Networks and Security: An Overview

A secure computer system network is the goal for every trustful business. Company owners and managers need to go to their houses and don't worry about being robbed or hacked during the night.

Correct network security must be able to prevent unauthorized access to the infrastructure, protect from misuse, modification, and destruction of the information that can be shared through the network. It must create a secure platform for the users and the instalment of safe programs.

Once you have installed a security system in your computer network, it should:

- Protect your programs and the web in general.

- Detect when there is an abnormal alteration in the system, as an unauthorized modification to the network.

- Take fast reaction when discovered the intrusion, to avoid damage to the system.

A security system is not only to stop the attacks but to prevent them altogether, making a strategy to cover every aspect of a possible issue.

Here are a few elements that should create a standard security system:

- Control the level of access to the network. Give passwords to authorized personnel only, and limit the different level of access that they can get depending on the job they do.

- Install anti-malware programs that would protect the network from most viruses, Trojans, and worms. These programs can detect hidden or dormant bugs that could be incubating and infecting all the system. Firewalls work as a preventive measure, reinforcing the work of the anti-malware.

- Securing your emails with programs that will block unsecured mails that may arrive.

- Use of VPN. By permitting authorized communication between the network and the computer, it prevents the entrance of unknown data, blocking if needed.

- Prevent human error by connecting your system to secure clouds, where the information can be preserved safely. That way, you won't need to use external devices that could be lost or misused.

Currently, there are dangerous threats on the Internet that can affect your computer network, and new ones appear every day. The most prominent are:

- Computer Viruses: They are tough to spot, and spread quickly if you're not careful. They can infect computer after computer, hidden inside the mail and downloaded archives. They can corrupt data, fill your computer with spam, even delete your hard drive without recovery.

- Adware and spyware: Both are programs that track your personal information and preferences on your searches; some adware is "inoffensive" and asks permission to be installed. They fill your screen with pop-ups, and your computer may work slower. Spywares are installed without you noticing it, and can steal personal information, passwords, credit card numbers, and more.

- Phishing: This is a dangerous program that retrieves personal information. They come in emails and instant messages that look "legit", and install a malicious malware when clicking the link in it.

- Trojan Horse: As the term indicates, a Trojan horse is a dangerous attacker disguised as a legitimate archive. They usually hide on emails, those with a familiar name for you, so that you won't doubt it before opening it. The Trojan hijacks your webcam and steals sensitive data that you may have safe on your computer.

- Computer worms: This dangerous malware spreads quickly through the computer contacts, infecting every other equipment connected to them.

These are just a few of the menace that you can find on the web, so it is crucial to managing good security for your computer network.

Advantages of a Computer Network

We use computer networks for social interactions, shopping and much more.

A computer network is a handy and valuable tool for centralizing and dispersing the stored information of a type of organization (companies, institutions, etc.). It is so vital in the contemporary world that we use them regularly without even realizing it.

Thanks to computer networks, we can locate all kinds of operations quickly and over long distances. Some of them are:

- Social interactions, teleconferences, video calls.

- Electronic purchase operations and capital movements.

- Data transmission, email and share resources in real-time.

- Transmission of stored audiovisual content.

- Satellite exploration and other surveillance and military recognition technologies.

Disadvantages of a Computer Network

The weak side of a computer network has to do with cyber-attacks, which violate the confidentiality of the information and can lead to dangerous activities.

We talk about malicious software (viruses, adware, etc.) or cyber-terrorists (hackers), whose attacks can cause loss of information (and therefore capital), threats to privacy or damage to equipment and software. The world of networks is diverse and complex.

Computer System Networks: Examples of Computer Networks

Here are some specific examples of computer networks:

- **A home network**: Like the WiFi, networks that anyone can install in their own home to serve a couple of computers or cell phones. Its scope will barely exceed the margins of the department.

- **A cybercafé**: The so-called cyber cafes were very popular with Internet penetration, before the arrival of Smartphones. They contain a series of computers that share their Internet connection and are available for public use. They were all framed in an internal network, whose head was the computer of the local manager.

- **A university campus network**: Also known as Campus Area Networks, these are actually MAN networks adapted to the various buildings and interests of the university community.

- **Internet. The biggest WAN available today**: communicating multiple technological devices over vast distances, from one side of the world to the other. This massive network involves computers everywhere, operating servers and workstations for millions.

Chapter Three: Computer Systems Network and Security

The Importance of Network Safety

A computer system’s network can be the improvement that your business needs to expand, but it can also be risky. If you don’t install a computer network correctly, there can be leaks that professional hackers can use to their advantage.

A high number of computers connected to the network means more possibilities to get infected, or have a security breach. If one computer is infected with a computer virus or a Trojan, it can damage and corrupt essential files and data. That corrupted information will also be corrupted in the other computers through the network.

There are other menaces that can affect the computers in your office or your home. The advantages of using a network to keep your computers and devices connected through the Internet can also be the biggest threat. They can share everything, and communication between them is fast, which means the threats spread fast too.

You can avoid most of these issues by installing firewalls and passwords to help prevent the access of malware and other dangerous digital programs. You will also need to be ready to fight them if they enter your network and make rules for every employee that will be using the web. They need to remember that it is for the benefit of all.

The Most Common Dangers for Computer Networks

Here are some of the most common threats you can find, what they are and what can they do to your computer systems.

- Phishing: It is a term used when referring to stolen identity. The malicious programs are hidden inside apparently safe emails, webpages, and more recently through messages. Once the user opens the contaminated archive, the programs are installed secretly on the computer or mobile device.

The e-mail usually looks like a piece of legal and urgent information for the user, disguised as a bank notification or a message from a real company. Once the program is installed, the cyber thief can obtain credit card information, passwords to bank accounts. It can even steal pictures that can be used for blackmail or other dark business.

- DoS and DDoS Attacks: The letters DoS stands for Denial of Service. The intention of these attacks is to crash a network, denying services to the users. It can be done by over-flooding the system with traffic, or the hacker can send a corrupted file that forces the network to shut down for maintenance.

The attacks are not meant for stealing relevant data or corrupting information. It is more to annoy the victims, making them lose money and time in fixing the problem. The intended victims are usually webpages of well-known companies, banks, commerce, or government, especially if they have very active online pages.

It also affects the frequent users of these websites that may need to reach some information and can't have access to it because of the attack.

There is another version of these attacks called DDoS (Distributed Denial-of-Service) attacks. They are stronger and harder to determine where it comes from because it uses several computers distributed throughout the globe. They infect the intended network with malware, thus overflooding it. The infected computers are called bot, and the cyber attacker gains control of them from a distance, creating what is called a botnet.

- Spyware: Spyware is malicious digital program or malware that infiltrates in the computer without your knowledge. It is one of the resources used for phishing, although it can be used in other ways. It copies personal data, like passwords and bank accounts. It also installs on your computer's hidden software to make changes in the configuration of your security information.

- Trojan horses: As the name suggest, a Trojan horse is a malicious program that infiltrates your computer disguised as a safe file. It can usually come inside an email with the name of a family member or a friend, to give you a sense of security that it is safe to open it.

The Trojan can also disguise itself as advertising, asking permission to access the computer. Real advertising is not malicious; that is why the Trojan horses hide in advertising that looks safe and legit. Once inside, they can corrupt your data or act as a spyware, stealing valuable information, and even cloning your webcam.

- Computer viruses: It is one of the most common dangers inside network security. As viruses do, they can incubate inside a computer, and spread quickly to all the computers connected to it. Inside a network, it is something to worry about, because it allows the virus to reach the other computers whenever you are trying to send an important file.

They can over-flood computers with spam, or change the configuration of your security system, making the network vulnerable to external attacks. It can also corrupt files from the inside and steal information. The worst of them are the periods of incubation. They can stay hidden and undetected on the computer until activated, and maybe it will be too late to do something by then.

What tools do you have available for securing your network?

If you want to protect your business network, you can use a varied number of tools available for you. The web offers an extensive range of services, and some companies give a guaranteed product so you and your company can be secured.

- Control of the access: When talking about security, you can't only focus on installing programs. Many security breaches can happen because of human error. An innocent or malicious employee can get access to essential data and use it with or without bad intentions, creating leaks.

If you want your network to be secure of these kinds of leaks, you must create secure passwords. They will allow them access to different levels of information depending on the user.

That way, it reduces the number of people that can access particular data, and leave fewer breaches for cyber attackers .

- **Analysis of the system behavior:** Whenever an application reacts differently to what it should, or software suddenly changes permissions, it will probably mean that some malware or other malicious programs have infiltrated the network. You can install software that will detect these changes and notify you before the damage is too significant to repair.

These kinds of software may not be able to prevent the attack but will help you and your security team to react faster and avoid irreparable problems inside the network.

- **Secure your email box:** Most of malware and viruses choose e-mail as their facade to infiltrate inside computers. To prevent the entrance of these dangerous threats, you must install a security software focused on the email box. This application will destroy or label the possible harmful files hidden inside the safe emails so that you can avoid them.

- **Firewalls:** These programs are one of the most used security tools. A firewall works as a barrier between your computer system network and external networks. It blocks the entrance to all unidentified or suspicious information that intends to enter your network, preventing the undesired infiltration of malware.

- **Antimalware and antivirus applications:** These programs search and destroy the dangerous malware that may be dormant inside a downloaded file.

They scan through the system continuously and send a notification whenever they detect an anomaly inside the software.Together with the firewall, antivirus and antimalware programs act as your digital soldiers to keep your information safe from thieves and attacks. They are active inside the network, so you don't have to worry when navigating through the Internet or when you open your emails. It doesn't mean that you don’t need to be careful when dealing with unknown emails and attachments .

- **Business VPN:** It stands for Virtual Private Network, and is one of the safest ways to protect your network. It gives private access only to those who you choose to enter your system, and they can do so from anywhere in the world. It is very secure because it is private, and is cheaper than installing a WAN network.

Some companies can offer you a business VPN service. The information and data sent through a VPN network are encrypted from end to end, which makes it harder to hack or steal. With a business VPN, you can also avoid international censorship applied in some countries, so that you can still have access to your business information from abroad.

Physical safety for your computer systems network

Keeping your hardware in good shape is as vital as giving protection to the software. Dust, heat, and liquids can be as dangerous as malware, or even worse. Information could be recovered from a corrupted folder, but there is nothing you can do with a burned motherboard. Here are a few tips on how to prevent physical damage to your hardware.

-

Cold areas: Computers generate a significant amount of heat. Most of them come with cooling devices, but these are not enough if the room where you keep them is also hot. Keep closed windows and curtains to avoid the sun's heat, and use air conditioners and fans to cool the room .

- Everything clean: These may sound like silly recommendations, but not many follow them. You must avoid eating and drinking in front of the computer and keep your area clean of dust. Bugs and mice can damage the hardware trying to reach the bits of food that may fall on the keyboards. You can spill your beverage on the computer and burn it. The dust can get inside the buttons of the consoles and damage the sensor, so a letter stops working. It can also get inside the cooling fan and affect it, overheating the CPU.

- Give maintenance to the computers: All the machines should be checked by a professional technician every few months. He can update all programs if needed, and also make cleaning of the hardware or recommend the change of a part if it is necessary. Maintenance is essential; it avoids further problems, which can be detected before they happen.

- Depend on the experts: If a problem appears, you should call a professional technician who knows about computer systems. You can try to do it by yourself and follow a tutorial, but you can jeopardize the computers guarantee. A computer system technician has studied to recognize a problem when it appears and will be able to detect the real issue once it checks the computer.

Some companies offer phone support for simple issues, and they can send someone to check if the problem seems to be more intricate.

The same goes with issues with Internet services and network installation services.

It is better to rely on a specialist rather than making things worse, trying to save time and money. The most probable thing is that you will end up spending a lot more.

Chapter Four: Computer System Network: Setting Up Your Own

What do you need?

Setting up a computer system network is very useful in every business. It makes communication between the computers an easier job, sharing the necessary data quickly and safely. Depending on the size of the network you want to create, you will need specific elements. Here is a list of the essential items you will need to start:

- Computer systems: You will need to have at least two computer systems to start a network. These can be a desktop or laptop, and they do not necessarily need to be in the same room. Other devices such as notebooks and tablets can be included in the network as computer systems. The network also connects the computer systems with computer accessories like printers, scanners, etc.

- Handy Tools: For some of the installations, you will need to have some tools. The most important one will be a screwdriver. If you can, use an antistatic wrist straps or be sure to have rubber shoes to prevent electric shocks. If it is a wired installation, you will probably need to have a drill to open holes and insert the wires so you can link the computer systems through the rooms.

- Modem with a broadband internet connection: This element is essential for a wireless connection, but it can also be handy for all the different installations. It provides Internet to the computer systems linked through the network, making it easier to communicate.

- Wireless Router and Ethernet cables: Depending on the kind of installation, you will need wireless routers or Ethernet cables to link the computer systems. For a wireless network, your computers systems should have a wireless network adapter. Most of the portable computing devices already have it installed on their systems, and even some desktops have one. If not, you need to acquire and install this device on your computer systems.

Types of Network

LAN: A LAN, or Local Area Network, is a network connection that is set in a specific area, like a house, an office or a building. Although computer systems don't need to be close to one another, they have to be inside the specific area. Currently, Virtual LAN is becoming more common when talking about setting up a network; wiring can take time and is more expensive.

Pros

- You can share information with other computers and computers accessories quickly. It makes it easier to send the final product to an output source like an external hard drive for storage, or print it.

- You can keep all the crucial data and information in one computer system. If you need to retrieve data from another computer, you can use a password and log in. It saves space and keeps the information secure.

- You can share a program license without having to buy one for each computer system. You don't even need to install the program on all the computers, connect directly to the main network through your device to use it.

- It is easy to install, and you don't need to be an expert. There are many video tutorials and webpages that explain how to make a Local Area Network.

Cons

- The network is limited to an area. You can’t work from home, or check information outside the building.

- You need to install a particular program to set up a LAN, what you need an administrator to keep everything going. It means it is a significant investment to do.

- If data is corrupted, it will probably be damaged in all the computers. An infected computer can infect the rest of them through the network.

WAN: A Wide Area Network allows to set a network without the limitation of area. It works excellently for companies that have stores in different regions of the city or other cities. You need to have access to the Internet to set up a WAN.

Pros

- You don't have the space limitation. You can have all the pertinent data in a central office, and manage all the other computer systems around the country. It helps communication between other locals, check inventory, and keep order without leaving your workspace or your home.

- It allows more advanced network technologies, setting exclusive passwords and software to make the net more difficult to hack or corrupt.

Cons

- It is costly because it requires specific connection plans, and the installation must be done in every workspace. You will need to pay monthly to have continuous internet service.

- It can be slow because of Internet traffic, and it can be interrupted if there are problems with the antenna that transmit the information.

- It needs continuous maintenance to secure that the software works correctly, and it has to be done by a professional.

MAN: MAN refers to Metropolitan Area Network. It is a net compound by smaller local area networks (LANs) and is used more like a network for a large area like universities. They can connect to the LAN of every building into a central system.

Pros

- It uses fiber-optic cable and other high-technology bandwidth to allow faster communication between the computer systems. Different departments can share relevant information in a few seconds; a file can be sent to a printer in another building. A massive memo can arrive in all the computer systems connected to the network at the same time.

- It allows economizing in the cost of Internet and other services, dividing the expenses between the users. At the same time, they all share a high-quality internet. It is not as fast as the LAN network connection but is faster than the WAN network.

Cons

- It is costly to install, and not all companies can offer this service. The technology it uses is the newest in the market. It can't use older installations, like other networks, so everything has to be installed for the first time, which means breaking walls and changing wires. It is a lot of work.

- You need to install first several LAN networks in the buildings you wish to connect, so it takes more time and investment to be done.

Setting up each type

Depending on the network, you may have to hire a third party to make part of the installation, while others can be done by yourself.

It implies knowledge of hardware installation to the search and setup of specific software.

For LAN:

- Once you have all the elements for the installation mentioned above, you need to select the central computer system. If it is the first time connecting the router to the computer, a "wizard" or installation helper program should appear and ask to create a network. If it is not new, go to Control Panel and look for the Network and Sharing Centre and select the option to set up a new system.

- If you want it to be a virtual LAN or if you're going to share the Internet between the computer settings, you then must set up the Wi-Fi. The manual of the router already has instructions for its installation. If you are not going to share the internet, go to the next step.

- Connect all the computer systems and computer accessories with a wire or through the wireless router. Some of the devices, like the printer, will need further instructions. In Control Panel, you will have to select Devices and Printers and click on the Add Printer.

Now you are ready to start sharing information in your small business or setting a game night with your friends in the house.

For WAN:

- You will need to have broadband Internet service with a company that provides it. These companies already have WAN plans to offer, so check which one would work for the kind of business you have. They will install the equipment in every building that will be connected to the WAN network.

- Connect the router to the WAN. This step usually is already made by the company when they install the service. In case they don't, you must find a router that can connect with that specific WAN circuit.

- Then it is time to connect all the computer systems to the router. You can do it via Wi-Fi, or use Ethernet cables to link the different devices. Do this process in all the stores or buildings that you want to connect to your WAN network, and you will be ready to start your business in other cities.

For MAN:

- To set up a MAN network, you need to have set a LAN network in every building you want to connect into one interface. You will also need to have broadband Internet service, optical fibers, and router devices to link all the LAN networks to a central system.

- Once you have followed the steps of how to install a LAN network in all the buildings, you must select which building will have a central computer system. There you will set the Internet service and the main router that will then interlink with the other routers in the different buildings.

Choosing the network for you

Each computer system network has its advantages and disadvantages. These reside mostly on the distances they can reach and the speed of the connection between the devices.

LAN: The LAN network is the best option for an office building and home installations. It allows setting many different computer systems, computer accessories, and other mobile devices into the same network as long as the devices are inside the area. You can share information faster than with other networks, link software and programs so the computers can work with it without having to install them in all of them, nor paying a license for each machine. It can be set up without hiring a professional. It can cover up an area from 100 to 1000 meters.

WAN: The Wide Area Network is perfect for business with multiple stores and branch offices. Whether they are in the same city or many cities around the country, it allows to keep track of the management of each store, so all the offices can offer the same service with the same quality. It can have a slower connection, but the information will arrive, making the communication safer. The range of the WAN can even reach to other countries, as far as 100.000 km.

MAN: The MAN network doesn't reach as far as a WAN, but reaches further than a LAN. It is best for universities or big hospitals, where they need to connect the different buildings and departments into one network. The internet connection is not as good as the LAN, but it is faster than the WAN.

The Metropolitan Area Network is the middle option between the other two networks, but it needs LAN networks to work. The range of the Metropolitan Area Network is between 50 meters to 100 km.

Chapter Five: IP And Subnetting Explained

What is an IP address?

An IP address is also known as an Internet Protocol address. It is a logical numeric direction or address assigned to every single computer, printer, router or any other device that is part of a TCP/IP-based networks.

The IP address is the very core component on which the whole networking architecture is built; no network exists without it. An IP address is known as a logical address that is used to identify every node in the network uniquely.

Because they are logical, they can change and vary. They are very similar to what we know as a town or a city because the IP address is that exactly, an address so you can communicate with other nodes or networks.

An Internet Protocol address is the most critical component in the networking phenomena that works to bind the World Wide Web together. This numeric address is assigned to every unique instance that connects with any computer communication network using the communication protocols, like TCP/IP.

IPv4 and IPv6, what do they mean?

IPv4, one of the core protocols for IP protocols today, was interestingly, also the very first version deployed for production back in 1983. We do see a fair bit of IPV4 traffic even today.

IPv4 uses a 32-bit address space, with a limited number of unique hosts.

We have to remember that Internet Protocol version 4 is a connectionless protocol and it operates on a best-effort delivery model. It does not guarantee delivery, and neither does assure proper sequencing or avoidance of duplicate delivery.

IPv4 addresses are represented in any notation expressing a 32-bit integer value.

IPv6, the newest Internet Protocol version 6, is the communications protocol that computers and networks around the world use for location, when accessing the internet.

As the number of Internet users started growing around the world, there was a need for more identification numbers. The IPv6 was introduced by the Internet Engineering Task Force, mainly to address the issue of a limited number of IPv4 addresses available. The aim, eventually, is to replace IPv4 completely. IPv6 was ratified as an Internet Standard on July 14 of 2017.

This Internet Protocol version 6 provides more technical benefits addressing the different network allocation needs and ensuring that there is optimal route aggregation.

These two versions of Internet protocol supported by manual IP assignment, can provide features of security inbuilt or optionally, and both have a Packet Header part. Moreover, both can transmit fragmented packets; both can have broadcasting and functions related to multicasting.

On the differences side, they tend to seem like two different things; ultimately; it is hard to assume that they are the root of the same tree.

IPv4 has a 32-bit address space while IPv6 has 128-bit address space. Also, IPv4 can provide 4.29×10^9 address while IPv6 can provide 3.4×10^38 addresses. IPv4 can support DHCP Address configuration. On the other hand, IPv6 goes a step further and supports auto and remembering address configuration.

While IPv4 does not provide end to end connection integrity, IPv6 can give purpose to end connection integrity, IPv6 does.

The RIP routing protocol does not support ipv6 while IPv4 is. Also, IPv4 is supported by SNMP protocol while IPv6 is not.

IPv6 doesn't have IP address classes while IPv4 is divided by categories like A, B, C, D, E.

IP address: public & private

A public IP address is one that can be accessed all over the Internet. Think about it like a postal address when it is used to deliver the mail to your home. A public IP address is the device address that everyone can see when they are searching for your device (or trying to locate it) online.

If you want to know what the public IP address is, you need to do a few clicks on your computer.

On the other hand, a private IP address is what devices within your private network uses. If you have multiple computers being used at your home, you may want to use private IP addresses to address each computer within your home.

In this particular scenario, when it comes to private IPs, your router gets the public IP address. Each of the devices connected to it is getting an individual IP address from your router via DHCP protocol.

Private IP addresses can only be guaranteed uniquely to an internal network. You also need a static IP address for the computer. Manually entering IP address will not work either.

To be clear, private IPs cannot be connected directly over the Internet like a computer with a public IP can. The situation mention enables an extra layer of security.

Setting up a computer network

These days, almost every small office has a local network and an Internet connection. To set up any computer network for your home or office, follow the following steps:

1. Wired or Wireless. The first thing you need to do is to choose between a wired and a wireless network. Wired networks use an Ethernet over UTP cable and tend to be faster when compared with a wireless network.

Also, wired systems are known for being secure and reliable. A Wired network doesn't work with devices without an Ethernet port like tablets and smartphones, and it is not easy and fast to set up thanks to all the running cables. Wireless networks, on the other hand, are straightforward to set up from the user perspective, and they allow easy access to mobile devices.

2. Components. Today, most offices networks use a wireless network or a mixed one. The main components required to start building an office network are:

- A router or wireless router that you can put pretty much anywhere in the house,

- A wireless access point,

- You also need an Ethernet HUB or Switch,

- cable cat 5 or cat 6 with RJ45 connectors

- Telephone cables with RJ10 connectors.

Also, broadband filters are needed too. For most networks, the wireless router or the Hub which connects the network to the internet will be the main component of the system and many times the only element. The wireless router has all the things you would want to get connected to the internet – including a wireless access point, an Ethernet switch as well as the DSL modem and router - all in the same box.

3. Router Location. The Wireless router will connect to the telephone line, cable or fiber network access point into the office or home.

So, the router needs to be located close to the main telephone socket.

The router provides wireless access and needs to be placed on a central location to get optimal results. Don't hide your router in a cupboard. Avoid installing it beside electronic machines and devices like motors or microwaves .

4. Test your signal. One of the easiest ways of testing your wireless signal strength in multiple locations is to use an app on your phone made to check your connection in various areas. If the signal is not optimal, try moving your router to a different location.

5. Extending the network. If the components are not enough for the space you want to cover, you will need to buy more parts.

6. Setup. To administer your router, you will have to access it via a web browser and login using a username and password that usually comes in the package where the router came. Before allowing devices to connect to your network, make sure you have edit or at least check the setup parameters of your connections.

7. Connect your devices.

What is sub-netting?

Sub-netting partitions a single physical network into smaller sub-networks or subnets. You get to see two segments, a network segment and a host segment.

Subnets were designed thinking about solving the shortage of IP addresses over the Internet.

An organization can use IP subnets for different reasons. For instance, you can use these to expand your network or address the varied physical requirements.

Sub-netting is also used by routers to make routing choices.

The subnet mask

A subnet mask, just like an IP address, has four bytes, and is what complements it.

To set up a subnet mask, we have to remember that it doesn’t works as an IP address. Instead, you will see that subnet masks come with an IP address. Yes, the two work together. For a subnet mask to become valid, its bits must be set to 1 on the left side of the subnet mask.

Setting up a subnet: how can you do it?

Some people may not need to set up a subnet if they only have a few computers in their network. Unless you are a network administrator, this process can seem a bit complex, and it is best to hire a professional.

Sub-netting works by using the concept of extended network addresses to individual computer addresses.

If a small business plans to use a specific network for its internal hosts, they use a default subnet mask. It allows everyone in the network to access the other device easily.

To subnet this network of more than 24 bits, it must be set to 1 on the left side of the subnet mask.

Exploiting subnets inside computer networks

Using subnets can improve network performance and speed. Sub-netting enables you to ensure that the information will stay in the sub-netted network and at the same time, maximize their speed and effectiveness.

Sub-netting also reduces network congestion by ensuring that traffic destined for a device within a subnet stays inside.

They also boost network security by splitting or dividing your network into subnets. You can control the flow of traffic using route-maps, enabling you to identify threats, close entry and target your responses quickly.

Chapter Six: Applying the Concepts of Computer Systems Network

Creating a computer network in your home

Creating or setting up your computer network at home is not as hard as it seems. It is quite easy if you put your mind and hard work to it.

The main reason why you may want to create a computer network at home is that you are looking for a better way to handle the Internet connection of multiple devices or computers.

The first thing you need to evaluate is the best type of network for a home.

You have two options, Wire Network and Wireless Network.

A Wire Network is more secure and reliable, but it doesn't work with devices that don't have an Ethernet port like tablets or smartphones, which is not convenient on a home nowadays.

A Wired Network is mainly used for network backbone, like connecting it to routers, network switches and wireless access points on different levels or floors.

When it comes to Wireless Networks, they work through Wi-Fi and are very easy and quick to install. A Wireless Network is generally slower when compared to wired networks.

They are easy to set up and allow easy access to mobile devices like smartphones and tablets, plus you don't have to run cables around your home .

The best type of network to create or set up inside your home will be the wireless network or creating a mixed network structure.

To set up your wireless network at home you will need a router or Wireless router, a wireless access point, Ethernet HUB or switch, some cables cat 5 or cat 6, a telephone cable and broadband filters.

Later on, you will need to figure out the best Wireless router location. It will need to be connected to the telephone line or fiber network access point in your home. The wireless router needs to be pretty close to the main telephone socket or you can change the location using a longer WAN cable. Try to keep your router out of cupboards, don't install it behind furniture or next to microwaves or motors.

Once you have your router location ready, you will need to test the signal to make sure the area is optimal. If it isn't, you can try extending your network with an additional wireless access point.

The last and most natural step is to set up your home router. You will need the username and password that usually comes in the box to administer it through a web browser or following the instructions on the box. It depends on the model and brand of the router. Once you are finished, enjoy your brand new home network.

But before we relax, we need to think about security and how much we need when we are working with a home network.

Since we are speaking about our home network, where we handle our most personal information, it is important to protect every connection made inside our house.

You can use a few tips to make your network as secure as possible.

First, change the name of your default home network. If you want to make your home network secure, you should change the name of your Wi-Fi network, better known as the SSID or Service Set Identifier. When changing the name hackers or malicious people out, there won't know what type of router you have, and it will make it a lot harder for them to understand how to attack you.

You should also make sure to set up a unique and robust password to secure your network. Having easy to guess passwords is never a good idea. An excellent wireless password should always be at least 20 characters long and include letters, symbols and numbers. You can search for different guides to set up strong passwords online.

The best thing you can do is activate network encryption to improve your Wi-Fi security.

Nowadays, Wireless networks come with multiple encryption languages, such as WEP, WPA or WPA2 and they encrypt all the traffic on your Wi-Fi network.

Creating a computer network for an office

When it comes to setting up the system for your office, the big choice doesn't rely on a wired or wireless connection, but on what you choose to use: switch or router.

A switch connects multiple devices on the same network inside a building. It enables connected devices like computers and printers to share information. Creating a small office network is not very comfortable without a switch to tie all the tools together.

A router, on the other hand, ties multiple networks together. For your office network, you will need one or more routers to help you connect your computers to the internet. With it, you can also connect computers to share one single internet connection. Think about it as a dispatcher.

If you have a rather small office, we still recommend sticking with a router.

Also, to have sufficient Wi-Fi coverage, you will need to have a wireless access point. Inside a small office is a good idea to have more access points with the signal strength turned down than to have one access point turned up.

For security, when setting your wireless access points, you should know that you also can set up a guest Wi-Fi network. Like this, you will only give your guest access to the internet but not to your internal network. It will ensure that your system will be safe from malicious attacks.

When selecting the right router for your office, keep in mind that you cannot compromise on the firewall. It’s what helps a router filter incoming cyber-attacks on your system. Plus, it’s a good idea to get a VPN too.

Creating a computer network in a large company

Today, every company works with its unique needs and priorities. We need the right network and network security to help team members to work and exchange information seamlessly.

To set up your computer network for your large company, the first thing you need to do is to define your requirements. Check how many devices you will need to connect to the computer network. Also, check the type of files you will be sending over the networks – file sizes do matter.

Look for the right software applications your team members will be using. Check if your employees need data.

The second but not less important step is to figure out if you should go wired or wireless for your business set up. For a large company, we always recommend a mixed network, where you enjoy the security and speed of a wired connection and the flexibility of a wireless network.

If you choose to go wireless all the way, the connection may drop out if you connect too many computers at the same time, and for a large company that will be happening a lot. That is the main reason why so many companies are choosing both wired and wireless network setups.

Once you have made your choice, the team needs to select the right hardware. Every business computer network, for instance, needs a router and a server.

You can choose a wired router as a getaway or wireless as an access point. You can also choose between two servers: either a cloud-based one that stores all your data online or a physical one that stores the content in-premise. The best option for a big company is a cloud-based server. A cloud-based server has a lot more flexibility, especially if you have big growth plans.

How does a Cloud-Baser Server Work?

‘The cloud’ might be a popular term but when it is combined with ‘computing’ things get big and a little complex. With the expansion of the Internet and portable devices, people now look to take their work everywhere. Cloud computing makes your work portable so that you don’t miss out on important projects.

The concept of Cloud Computing

Suppose you are working on an assignment and wish to send it to a team member for proofreading or checking. You wouldn’t like to copy all that data into a pen drive or a portable hard disk and go all the way to deliver it, would you? Email can be a useful tool but fails to work when the data is beyond 25Mb. This is where cloud computing kicks in.

Cloud computing involves use of computer resources that are connected with a localized server of desired specifications using a data connection preferably over a wireless network. In order to gain access to the server, one needs to have a dedicated application with every user possessing a password. Apple’s iCloud is an example of cloud storage that allows users accommodate data on a centralized server that can be accessed using any compatible device.

The trend of cloud computing is fast catching up thanks it its flexibility in use and the kind of convenience it offers to the consumers.

What makes cloud computing different from traditional server-based systems?

The architecture of a cloud computing system isn't as easy to implement as it appears. The perfect cloud can only be effective if done by the right team of professionals. So, how does this interconnected system work? Most websites and applications run on massive servers that are capable of handling large amounts of data. What makes websites different from a cloud based system is the fact that the cloud utilizes resources of discrete devices to form a large virtual computer.

Cloud computing reduces the dependence on a single hardware or a software resource. This makes it easier for companies to host websites. For instance, if you are hosting your organization's website from a local server that supports only Windows OS, you are tied up to that OS all the time. On the other hand, if the site is being hosted on a cloud, multiple platform programs can be run without any issue.

Implementing cloud computing network – The Architecture

This network comprises of 2 primary components – the infrastructure and the cloud platform. These can also be termed as the back-end and front-end layers. The back-end layer of a cloud computing network consists of the hardware, memory as well as software that is used to run it efficiently.

The front-end of the network has the cloud platform which is where the users interact with the entire network. The cloud platform is basically a web-based application with multiple utility options.

Pros and cons of Cloud Computing

Cloud computing provides an excellent platform to share information without having to compromise of resources besides being cost-effective.

However, some IT professionals believe that deployment of cloud computing may cause serious security breaches. Nevertheless, these issues can be dealt effectively with the help of deterrent, preventive and corrective controls.

Cloud Services for your business

There are a truckload of companies offering you cloud storage for free. While many cloud based services like Google Drive and Dropbox offer some GB's of storage for free you can even subscribe to their monthly plans – to suit your business needs. Organizing files, sharing data and working together become a whole lot easier when you use the cloud technology.

When choosing the right routers, opt for the ones that allow you to enable your VPN server and provide employees with safe remote access. Also, you can select one that includes added security features like anti-spam features.

Keep in mind that while you and your team are choosing for a database system, you need to define your looks and remember what type of business is going to use the network setup.

To protect your business network, make sure to use a WPA2 or an encrypted protocol for passwords on the router.

Another way to protect your business network is by disabling or restricting the DHCP. The DHCP defines what IP address the devices on the system will have.

Moreover, make sure to use a VPN or virtual private network to encrypt the internet connections and data transferred through your system.

To have an even more protected network, always update router firmware so your business will not be vulnerable to attacks due to outdated router firmware.

To ensure the security of your network, also disable the file sharing option. This should only be enabled on file servers. If you don't do it like this, the files that your team shares will be seen by every user on the same Wi-Fi connection.

Creating a computer network in a school

When it comes to creating a computer network for a school, we need to think about computer labs and a lot of database systems. It is highly relevant to set up everything right so the educational environment will be secure and working correctly.

If we are going to set up a computer network for a school, the best we can do is choose a wire connection. This way, we can ensure that the connection will be secure and fast, and at the same time, the kids won't be stealing the Wi-Fi passwords and connect to the network with their smartphones.

In these cases, it is also better to use switches instead of routers. So, we can make sure that every device is connected correctly to each other.

When choosing the right database system for a school network, it is essential to check the following points: the integrity of the data, the performance and the ease of maintenance.

If you choose a server-based database system, you will have built-in protection against corruption on your data and files.

Shared-file databases are slower than a server-based system, mainly because each user is reading the whole data over the local area network. So, it is better to go with a server-based system which enables the server to compute and return the answer quickly without pushing large chunks of data over the network.

About the security measurements, make sure to enable the WPA2 or encrypted system, make sure to allow a VPN and protect at maximum the connection of the network.

It is essential to install a web application firewall for extra protection and always update the router firmware to avoid attacks.

When it comes to school networks, it is a must to disable the file-sharing options and only use it on file servers. So, the information can be secure and not on every single computer inside the network.

Chapter Seven: Outside the Network Numbers: What Still Matters

The outside can still harm your networks

Network security shouldn’t be focused only on the internal threats that can affect the software and corrupt or steal all the relevant data inside your computer systems. There are harmful external elements that can also damage the physical components, especially to the infrastructure of the network.

These threats must not be taken lightly. Virus and malware can be avoided using diverse programs, but a sudden blackout can burn the computers and all-electric elements of the network. A flood on a room can damage the cables inside the walls of the building or house.

External elements can affect either LAN, WAN or MAN networks all the same. Bolts of lightning during a storm can damage the antenna that connects the buildings between them, breaking the link that keeps the network together. Birds on the roof or mice and bugs in the walls can also be a potential threat.

And you must never forget the human factor as a possible problem for your network. Humans make mistakes and can damage the network in unexpected accidents. There are ways to protect your computers system network from most of these possible issues, the same way you can protect it from internal problems.

The location of your network

Currently, most of the LAN networks and all of WAN and MAN networks depend on a considerable measure of Internet connection. Without it, you can’t link computers far away from each other. Many companies can offer this service, and even some of them have special plans for WAN networks. They give exciting prices depending on the number of stores you will connect.

These companies are called Internet Service Providers or ISP. Depending on your country you may have a handful of them, some of which offer other services like phone service and satellite television connection. The company provides service through ADSL cables that go around the city, or an antenna installed on the roof of your building or house.

The antenna signal can be affected by other signals, the microwaves crashing to each other and making it difficult to connect. Your broadband internet connection can also be changed depending on how far from the primary source you are, or how many repeater antennas are in the area.

The most common problems are slow speed on your Internet and intermittent signal, which makes the network unreliable. If the computer systems are too far from each other, the connection could not be as secure.

Choose the location for your network carefully, and inform yourself about the best ISP companies you can find whether they are local or a widely known company.

Buildings and construction materials

You may have found that the potency of the Internet signal may vary in different rooms of your house or building. These problems are probably because of the materials of the walls and roof of the structure. They prevent the signal to reach effectively to every room. This issue is not suitable for an operative computer network, forcing you to choose specific places to place your computers and mobile devices to work correctly.

One of the most common materials for construction is concrete, which is used for a strong foundation for houses and buildings. But concrete is also the material that blocks Internet signals the most. It is the reason why is hard to have Internet connections in basements and underground garages. Concrete comes in different versions, like reinforced concrete that has metal in their composition. The thicker the concrete is, the harder it will be for the internet signal to reach the computers.

Clay brick wall constructions can also block a certain amount of signal but is not as strong as the different kinds of concrete. Masonry blocks are also used very frequently. Although they don’t block the signal as the concrete, they do prevent the free movement of internet signal.

Lumber walls block less signal than clay bricks, making cabins and other wood structures a good option too. Glass blocks a little signal and that is why the Wi-Fi connection on mobile devices work better close to a window.

Finally, plywood and drywall don’t block any signal, making them the best materials for walls inside an office building.

The best way to secure a good computer system network is to place the router in a middle point inside the house or building that can reach many rooms at the same time. Also, you can add some routers in the other places that can repeat the signal to those rooms with thick walls and that are located far away from the main router.

For LAN connection this problem can be solved using Ethernet cables instead of a Wi-Fi connection in the interior of the house or building, which is faster. That way, you can put your primary computer on the basement, making an internal cable installation that will allow the computer to connect to the upper floors. This measure allows a safe connection, making it harder for other external problems to reach it.

Weather

ISP companies can offer one of the following services, or both of them: internet by ADSL cable, or by satellite signal. ADSL cable internet is faster than satellite Internet, and it connects the network directly between the computers. At the same time, these cables are more likely to suffer from external elements like rain and strong winds that will make your connection unstable.

Cold and rainy environments can affect the electromechanical switches and breakers, provoking blackouts and damaging the electrical machines. Hot weather can also affect the hardware and electrical element of a computer network, overheating the cables and melting metal components. It can provoke dangerous electrical short circuit.

Although most of the ISP work with copper wire cables, some are starting to use optical fiber cables.

They are safer and avoid environmental damage in a more effective way. But these cables are not cheap so that the service can be pricier than other companies .

One of the most dangerous environmental threats are lightning during a storm that can fry all the circuits. They do not even have to reach the antenna to affect the network. Lightning is attracted to magnetic material, like copper wire cables. The best you can do during a storm is shut down all your electrical elements, unplug them, and wait until it is over. You shouldn't risk it because the physical aspects of your computer network are very delicate, and this kind of problems can give you quite a headache.

The best weather for a computer network is a beautiful cloudy day without a hot burning sun in the sky, neither strong winds that could affect the cables. Storms should be avoided at all costs, taking the correct measures to prevent damage to the network. You can't avoid the possible problems to the wired system in the city, but you can protect your assets the best you can. That way you won't have to buy a new one, and remember that information can't be recovered from a burned motherboard.

Human interaction

Finally, the most common and frequent threat that all computer networks must face is human error. People can be negligent and take everything for granted. Many haven't received correct education on how to interact with computer systems, or don't care about the consequences. Whether it is done unintentionally or with malice, there is danger in the contact of humans with the network.

Forgetting to protect your equipment from environmental problems is considered a human error. In practice, all the issues mentioned before are somehow related to humans. This and many other problems are part of the lack of education that many workers and employees usually have. Some may have never worked with a computer before or are used to be less careful with their computers. Here are some of the most common problems that can happen because of human interaction:

- Downloading viruses and malware: The security system can detect, notify, and put in quarantine the files and data that may be infected with viruses or that have malware attached. It is up to the user if they decide to open the file anyway. Security breaches are frequently done by employees that open e-mails and click on fake links, ignoring the warnings that the computer system gives.

Some employees use the work computer as their computer, getting in unsafe websites, or opening their mailbox during work hours. This behavior allows the viruses to spread through the network, affecting all the computers connected to the infected one.

- Changing the settings: Some people like to mess with the configuration on the computer trying to make it work as they want without really knowing what they are doing. Changing the settings can affect the functionality of some programs and software, which can affect the data inside the network or provoke leaks and security breaches.

An excellent way to avoid this problem is allowing only administrators to access the settings panel, putting passwords to prevent unauthorized entrance. Still, it is best to give the appropriate warnings to the employees about the settings. A professional technician should do any change and installation of software.

- Liquids accidents: People are so used to computers as a daily tool that they forget how delicate they are. It is a commonplace to see employees eating and drinking in front of their computers, unaware that they could have an accident and spill the drink on the keyboard or worse, in the CPU.

These accidents can result in the loss of a monitor or a keyboard, having to replace the damaged asset. But it can also mean the destruction of relevant data inside the computer system, unable to recuperate it.

- Leave everything on: This error is frequent not only on employees but also managers and owners. Even if it looks like you can save time leaving the computers on once the work hours finish, it is dangerous. A blackout can damage the circuits and burn the networks components. You can use a regulator to avoid most of the damage, but the best to do is turning off and unplugging the computers before leaving.

A good education about computers and how to treat and maintain them should be able to help avoid these problems. It would be a great idea to have a meeting every few months to remember the employees and also the managers and head of departments the importance of taking care of the computers.

Notably, workers must remember that computers are part of the company's network, and not their personal property. They must be extra careful with these essential assets because it is one of the most important tools in the business. Keep the rules in places where they can look at them and keep them in mind. They can even learn to apply these rules in their houses.

Conclusion

The next step is to analyze and digest all the information here provided. Computer system networks can be easy to understand at first; setting up a home network is an easy task—even more so when you're using LAN structures.

However, to fully exploit their advantages, you can apply them to your business, regardless of what it is.

If you have a clothing store, you can use the networks to communicate databases, inventories, store traffic, or even communication between all stores.

Of course, their usefulness increases exponentially as your ventures move towards technology and communications. With that usefulness also comes complexity.

Computer networks provide a plethora of benefits, and these increase with their versatility. That versatility requires a lot of studying and practicing.

Therefore, the best next step is to look for additional resources or a future book delving into the more advanced concepts and procedures. Whether you want to work as a computer systems network expert or simply hire this service, you need to understand how far it can get; then, you need to understand how to get there.

As a last piece of advice, we're leaving additional resources at the end of this book, so you should look them up and internalize all the information contained in them.

For aspiring specialists, the best way to get into the business is to prepare yourself before pursuing a career. That way, the road becomes much simpler, and you can practice beforehand. Entering the professionals market will be less harsh once graduated as well.

For entrepreneurs looking to exploit these concepts, it’s also an excellent idea to read further on the topic. That way, you’ll know what you want on your personnel; you also skip having to depend entirely on them.

So, that’s it: the next step is to learn more and make sure you understand all the information contained within. Try setting up a network in your house or office as a test!

Resources:

Chapter 1:

https://collegegrad.com/careers/network-and-computer-systems-administrators

https://en.wikipedia.org/wiki/System_administrator

https://www.techopedia.com/definition/25597/computer-network

https://www.genesee.edu/academics/programs/IT/csn/

https://www.bls.gov/ooh/computer-and-information-technology/mobile/network-and-computer-systems-administrators.htm

https://www.careerexplorer.com/careers/computer-systems-administrator/

https://www.careerexplorer.com/careers/computer-systems-administrator/how-to-become/

https://www.careerexplorer.com/careers/computer-systems-administrator/

https://www.bls.gov/ooh/computer-and-information-technology/mobile/network-and-computer-systems-administrators.htm

https://pandorafms.com/blog/how-to-be-a-good-sysadmin/

https://www.business.org/hr/recruitment/traits-look-hiring-system-administrator/

https://pandorafms.com/blog/how-to-be-a-good-sysadmin/

https://www.inspiredtechs.com.au/computer-networking/

https://www.ableone.com/four-benefits-networking-computer-systems-business/

Chapter 2:

https://peda.net/kenya/ass/subjects2/computer-studies/form-1/the-computer-system

https://www.techopedia.com/definition/593/computer-system

https://study.com/academy/lesson/what-is-a-computer-network-types-definition-quiz.html

https://www.britannica.com/technology/computer-network

https://whatismyipaddress.com/ip-address

https://www.techopedia.com/definition/2435/internet-protocol-address-ip-address

https://www.techopedia.com/definition/28328/subnetting

https://www.csoonline.com/article/3285651/what-is-network-security-definition-methods-jobs-and-salaries.html https://securitytrails.com/blog/top-10-common-network-security-threats-explained

Chapter 3:

https://securitytrails.com/blog/top-10-common-network-security-threats-explained

https://www.theamegroup.com/5-common-network-security-risks/

https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html

https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos

https://us.norton.com/internetsecurity-how-to-catch-spyware-before-it-snags-you.html

https://www.forbes.com/sites/forbestechcouncil/2018/11/15/what-is-a-business-vpn-and-how-can-it-secure-your-company/

https://business.bt.com/help/guides/vpn-for-business/

https://www.cisco.com/c/en/us/products/security/what-is-network-security.html

Chapter 4:

https://www.quora.com/What-are-the-advantages-and-disadvantages-of-metropolitan-area-networks

http://www.tribuscomputer.com/lan-vs-wan-the-pros-cons-of-each/

https://searchnetworking.techtarget.com/definition/local-area-network-LAN

https://techsolutions.cc/security/guide-wan-vs-lan-vs-man/

http://www.itrelease.com/2018/07/advantages-and-disadvantages-of-local-area-network-lan/

https://www.wikihow.com/Set-up-a-Computer-Network

https://www.broadbandchoices.co.uk/how-to/how-to-set-up-a-local-area-network

https://smallbusiness.chron.com/build-wan-28601.html

https://www.conceptdraw.com/How-To-Guide/metropolitan-area-networks

Hacking

A Quick and Simple Introduction to the Basics of Hacking, Scripting, Cybersecurity, Networking and System Penetration.

Hans Weber

Introduction

If you ask someone what hacking is, they will typically tell you that it is someone that penetrates the security of a system and gains access to it. That is surprisingly not what it always meant. The word "Hacker" was initially used to refer to anyone that was a skilled programmer, but due to popular cultural representations, the definitions have changed over time. So let us dig deeper into some basics of hacking and try to explain the culture, the misunderstandings, and the technicalities.

What is a Security Hacker?

When we refer to a hacker, we are typically talking about a security hacker. A security hacker is a person who can exploit an existing computer or network system and is able to use it for their personal motives. To further understand the motives of hackers, we have to look into the different types of hackers that exist and how they use the information or power that they gain once they have accessed a system.

The Different Kinds of Hackers:

Among the many kinds of hackers that exist, there are three that are popularly depicted through the media and are popularly referred to. They are as follows:

1. **Black hat hacker**: A hacker who has malicious intent
2. **Grey hat hacker**: A hacker who has good intent but hacks without seeking permission

3. **White hat hacker**: A hacker with a good intent that seeks permission before hacking

We will be looking at each of the classifications in detail in further chapters.

Other Classifications of Hackers

There are other ways that security hackers are classified. These include classifications by the skills of a hacker. Some of the following are commonly used skill-based classifications:

1. **Elite Hacker:** The most skilled hacker having extensively exploited systems
2. **Script Kiddie:** A hacker that lacks experience and uses pre-written scripts
3. **Neophyte (Newbie/Noob):** A hacker who lacks both knowledge and experience

How Does a Hacker Hack into a System?

When hacking into a system, a hacker follows a number of steps to ensure that they can enter and use the system as they require. These can be broadly categorized into three separate subheadings, which are as follows:

1) **Network Enumeration/Reconnaissance:** Network enumeration is the first step of hacking. It involves getting acquainted with the system and networks that the victim is using. This usually involves retrieving sensitive data about the network,

including the usernames and information of members that use the network, as well as their email addresses. A hacker typically downloads the entire website. Overt discovery protocols are used for this step of the procedure .

2) **Vulnerability Analysis:** After having carried out a network enumeration, the hacker now knows the people and entities that are a part of a network. The next step is to find the vulnerabilities within the systems that are connected to the network. This allows the hacker to enter the network by exploiting the vulnerabilities that he may have found. Many tools, such as vulnerability or a port scanner, exist to allow a hacker to analyze vulnerabilities within a system quickly. A hacker may also manually test vulnerabilities by looking for automated emails and the email server that is being used by the staff.

3) **Exploitation:** The final step of hacking comes in the form of exploitation. Exploitation refers to overpowering the vulnerabilities to make the software or network act in an inconsistent manner. This is typically the stage that most people refer to as "hacking," and we will look into it in extensive detail when we discuss cybersecurity.

After having actively hacked into a network, a hacker tries to maintain a low profile. They can do so by accessing accounts that have not been used for a long time, or making an admin account for themselves and trying to blend in. Hackers also typically attack after having changed their IPs and machine codes to ensure that there is no track of their activity left. If no one notices the new staff member on the site, the hacker has successfully blended in and can continue to do as they wish on the site. That is why it is important to keep track of your staff members and ensure that they aren't "ghost" members.

How to Keep your Network Safe

Now that we know how a hacker manages to access a system or a network, we can logically conclude ways to ensure that the hacker is unable to get into it. The first one is obviously to ensure that your staff members aren't traceable, and vulnerabilities don't exist within the website or network that you run. Unfortunately, that is not as easy as it sounds, and vulnerabilities continue to pop up in all sorts of networks. This includes high-profile tech companies, including Apple and Facebook. That is why it is important always to ensure that you have the updated version of the apps. Updates typically exist to resolve security issues or other bugs.

So you might be wondering, if big-tech firms like those are unable to keep themselves safe, how could you? Well, the answer is pretty simple. While it may not be possible to close off all vulnerabilities, it is possible to train your staff. Ensure that you keep a good check on the members of your network, immediately see the history of any anomalies and take action, and train your staff never to leave their emails vulnerable or ghost accounts standing without informing the management of the network. That way, you will be able to ensure that no hacker manages to exploit any vulnerability that they may find, and all threats are promptly taken care of.

What Can Be Hacked?

It is a common misconception that only systems such as computers can be hacked, and everything else is typically safe. The fact is that anything and everything that is connected to a network can be hacked by exploiting the network itself. While a complete list would be exhaustive, some of the things that can be hacked include baby monitors, smart TVs, thermostats, printers, and cameras. In a now-famous incident, someone hacked into 50,000 printers and made them rapidly print out messages asking people to subscribe to Pewdiepie.

Can a Network be Un-Hackable?

While there are a number of ways to make your network secure enough to deter hackers from trying to enter it, there are no websites or networks that can prove to be unhackable. Even secure networks such as the NSA have been hacked at one point or another. A popular Reddit thread lists all games that call themselves "unhackable," followed by a general challenge to hack them. All of them eventually got hacked.

Chapter 1: Black Hat Hacking

Now that we know the basics of hacking well, we can dig deeper into the motives of certain types of hackers and what they aim to do by making their way into a system. Any such list obviously starts with the black hat hackers, popularly depicted as villainous typists that work on a black screen, by media.

Motives of Black hat Hackers

To understand the operations of such hackers, it is important that we understand the motives that they have when trying to hack into a system. The motives are usually broadly tagged as personal gain but can be categorized into a number of classes. Typical motives can include the follows:

1) **Blackmailing:** While blackmailing is not an ultimate motive, it is usually what encourages a hacker to hack into the data. By getting access to the data, they are able to blackmail the owner and gain personal benefits. These include financial gains as well as making the person being blackmailed oblige to a request.

2) **Financial gains:** Financial gains can be achieved in a number of ways by black hat hacking. We have already discussed that people can be blackmailed to get money. Other ways of gaining financially include selling the personal that the hacker manages to steal, and working for a third party and getting paid for the hacking services.

Hackers can also hack directly into your bank account and take your funds!

3) **Revenge/Fun:** While typically not the motive of skilled hackers, novice hackers may hack into the data of a person simply for fun, or for some form of revenge.

4) **To practice hacking:** A typical black hacker that is still learning may hack into a website and make it unusable simply for practice, to enable themselves to target bigger and more secure networks in the future.

The Harm of Black hat Hacking

There are a number of harms that we are exposed to when we are targeted by black hat hacking. Contrary to their white hat alters, black hat hackers typically lack moral responsibility and thus take little to no care of how the data that they are hacking is being used.

This means that while a hacker may have hacked the data for an entirely different purpose, having gained access to it, they might just leak it to the internet. Marketplaces in the dark web typically buy such data, making it public knowledge. In a recent attack, someone leaked 773 million emails and 21 million passwords online. With breaches at this massive scale, we should ensure that we keep our passwords secure so that no one can gain unauthorized access to our accounts.

Other than leaking your data online and allowing anyone access to your account, there are other harms that come with black hat hacking. The first of these would be a financial loss. In the case of being blackmailed, you might choose to pay money against having your privacy being compromised. By hacking into your bank data, they can also easily transfer funds from your account into their own, and thus rip you of your money.

Black hat hacking is particularly dangerous for those who run servers or networks. A black hat hacker would have little care when trying to enter a vulnerable system and can thus use extreme methods to ensure that they get control. That not only means that they might render your site or network useless for the time, but also that they might take over the ownership of the site and use it as they wish, stealing yours, your staff's and your customer's data. That is why it is important that any attempts at hacking are promptly dealt with, and security is tight enough to discourage any hackers.

The Legality of Black hat Hacking

Hacking itself is not illegal. That is because there are a number of ways in which hacking can promote good within society. However, given the work that black hat hackers do, their hacking being non-consensual, their operations are illegal. While laws greatly vary with country, depending on the severity of the case, black hat hackers may find themselves facing years of jail time and thousands of dollars in fine, as well as payment for any damages, caused. We have seen some cases where hackers have received as many as 90 years of jail time.

Chapter 2: White Hat Hacking

In contrast to the black hat hackers that seek to exploit vulnerabilities of a system for personal gains and break laws in doing so, white hat hackers follow the laws and hack only with consent. That does not, however, mean that the hacking itself is not for their personal gains. Let us explore how these ethical hackers operate and what their motives are.

Why do White hat Hackers Exist?

White hat hackers surprisingly exist because black hat hackers do. If there were no black hat hackers, no white hat hackers would be needed to check the system for flaws and vulnerabilities. White hat hackers primarily get the consent from a network admin and try tap or hack into their network. If they are successfully able to do so, they tell the vulnerabilities within the network to the admin and may offer to help them close any such vulnerabilities. The role of the white hat hacker is the exact opposite of the black hat hacker, and they aim to protect and secure a system. The methodologies that both kinds of hackers use are the same, though.

Motives of White hat Hackers

So you may be wondering why someone would want to hack into a system with consent to find vulnerabilities.

There are a number of reasons that white hat hackers would do so, and we are going to list some of them below:

1) **Securing their Network:** Hackers are typically very skilled programmers and might own their own website or network. They might attack their own network with the motive of finding vulnerabilities and securing them, to ensure that no one else can gain unauthorized access into it.

2) **Financial Gains:** White hat hackers, particularly the good ones, are paid high by companies that wish for the flaws and vulnerabilities in their systems to be closed. Thus by being a white hat hacker, a person can earn a large amount of money through being paid for the services that they offer.

3) **Social Service:** A hacker might wish to provide a social service by raising awareness about data security. They could thus work with companies for free and show them their vulnerabilities.

4) **Learning:** A newbie hacker may offer their services for free in a bid to learn. If a white hat hacker is able to hack into a complicated and secure system, they are typically offered better payment packages earlier in their careers.

A typical white hat hacker can earn a lot more money than most careers have to offer. Many companies offer thousands of dollars for anyone to identify any vulnerability within their network and might offer more for that person to fix them.

Benefits of White hat Hackers

The benefits of having white hat hackers are many fold, and the most important one is to find vulnerabilities within a system. When a white hat hacker is able to identify the problems within a system, they are quickly fixed. This means that when a black hat hacker tries to hack into the system, he will find that the vulnerabilities no longer exist, and would thus be unable to do much damage.

In an ideal scenario, this should ensure that no black hat hacking occurs. However, there are a number of issues with that. First of all, not many networks hire white hat hackers. That means that they are left open to the vulnerabilities that exist within the system. To add to that, some black hat hackers may be more adept than a white hat hacker and may be able to find vulnerabilities that the ethical hacker missed out on, which means that the system is still open for flaws. That is why we should never let our guard down.

Earnings of a White hat Hacker

A white hat hacker can typically earn a median salary of over 80,000 dollars. Each assignment can earn anything from 15,000 to 20,000 dollars, and the best bounty hunters can manage to earn as much as 500,000 dollars a year.

The Legality of White hat Hackers

White hat hacking is legal, as it does not break any of the laws and is done with consent.

White hat hacking is thus considered a reputable career and can bring you big earnings, and is legal on top of that. If one wants to learn hacking and system penetration, they should try and go for a white hat hacker profession .

Chapter 3: Grey Hat Hacking

Laying between white hat and black hat hacking is grey hat hacking. While typically it was not recognized, it has now become a huge part of the hacking industry and is thus given more notice. Grey hat hacking is technically ethical hacking, and the person engaging in it has no malicious intent and does not intend to steal data or blackmail someone. They also, however, do not seek consent before engaging in the activity and are thus put in a "grey" spot between black and white hat hackers.

Why Would Someone Engage in Grey hat Hacking?

While the motives of most white hat and black hat hackers are clear cut, people in the grey area are harder to read. Nonetheless, there are a number of reasons that we can identify for which someone would want to engage in grey hat hacking.

1) **Financial Gain:** The primary reason that people engage in grey hat hacking is for financial gain. When being unable to find jobs as a white hat hacker, they typically hack into a vulnerable network and tell the company about it, seeking monetary rewards and to be hired to fix the vulnerability. Many companies now tend to report such activities, though, and that means that financial gains have minimalized.

2) **Learning:** When you're a hacker, the whole web is your platform. Learning hackers that wish to engage in ethical hacking in the future might feel that they need to learn by hacking into random sites. While no malicious intent exists on their part, it is still illegal. A number of sites now offer hackers to attempt to hack them for learning purposes, removing the need to learn using illegal means.

3) **Activism:** Perhaps the most widespread usage of grey hat hacking is for activism purposes. This type of hacking is now coined as red hat hacking. We will dedicate a separate section to exploring this form of hacking.

The Legality of Grey hat Hacking

Grey hat hacking is not legal. The legal implications are typically the same as those in the black hat hacking scenarios. However, given that most grey hat hackers do not seek to harm a site, and at times only wish to help, the incidents are typically not reported at a high rate, which means that grey hat hackers are not always punished. That tends to encourage the activities of such hackers.

The Curious Case of Kevin Mitnick

No story of grey hat hacking is complete without the mention of Kevin Metnick. Having started hacking into systems at a young age of 12, Kevin had managed to hack his way through many high-security systems, including Motorola, Netcom, and Nokia. He had over a hundred spoof cells and codes that he used to hide his location.

He was soon listed as the most wanted hacker and subsequently sentenced to 5 years of jail time.

After having served jail time, Kevin turned over a new leaf and moved from grey to white hat hacking. He wrote multiple books, many of which went on to become bestsellers. He now works with many of the Fortune 500 companies and helps provide them with solutions to their vulnerabilities.

Kevin is now one of the best-known hackers in the world, and his story shows us that grey hat hacking, despite how safe it might seem, is not legal or encouraged. If you feel that you have a knack for hacking, you should go team white!

The Controversial Red Hat Hacking

Red hat hacking is currently branched under the umbrella of grey hat hacking. It is more popularly known as hacktivism and is a prime spotlight of the innovations to hacking in the 21st century.

Hacktivism is typically used as a form of activism, and the hacker uses hacking to draw public interest to a matter of global concern that should be taken note of immediately. Groups of hacktivists exist, including Anonymous.

One of the prime activities that Hacktivists have engaged in is the deletion of sites that display child porn. By gaining access to those sites and deleting their content, they have managed to clean the internet of illegal and immoral content.

WikiLeaks is a depository of documents that were obtained using hacktivism measures, including many state and national secrets that the hackers believe people have a right to know. As many as 400,000 documents about the US war on Iraq exist on the WikiLeaks server.

Hacktivism is typically illegal since it involves hacking into websites without consent, but it may be considered legal when the hackers hack the deep web to remove problematic content from it.

Chapter 4: Networks

No book about hacking is complete without a mention of networks. If a computer system or data is stored solely in a system with no network connected to it, the hacker would only be able to access it if they were able to access it physically. It is due to networks that hackers are able to enter a system and get access to the data.

What is a Network?

A network is a system in which different entities are connected together. A computer network is no different and consists of interconnected computers that share information with each other.

How are Networks Connected?

Networks are connected and made through a number of ways. Some networks may be connected to each other using the common copper wires that we see being used for the slower internet modems. Other networks are formed through the more solid fiber cables with faster connection speeds. Networks don't need to be hooked together at all and can be formed through all the devices connected to single Wi-Fi.

Types of Network

There are two broad types of networks. The first type is a Local area network, also known as a LAN. The LAN typically connects entities within a small distance and includes simple systems such as those in a company where all the systems are connected to one another. A simple benefit of using the LAN network would be better utilizing the resources. By using a LAN network in a company, you can make your job easier and save space.

How it works is that you would have one computer dedicated to storage. It would store all the files as well as all the software. The other systems can simply use the resources from the storage system, which means that the files and software do not need to be in every computer in the system.

The second type of network is the WAN network, also known as the Wide Area Network. This is a non-internalized network that connects one entity to outside entities. It thus connects all LANs to one another, letting them pass information between one another. The Internet is a WAN and connects almost all servers in the world in one way or another.

The internet does operate in a way similar to the LAN networks. All the files that you require are contained on the internet, which means that you don't have to go out and locally seek images, text, software, and information. However, access to the internet, or any network for that, does leave you vulnerable to the problems associated with hacking since someone can tap into your network and steal your data.

This is why care needs to be taken with any network that is connected to a network in any way.

Are We Safe if We Never Connect to a Network?

While it is typically not a choice, given how everyone in today's world does need access to resources that you can get from the internet or other sources, let us assume that a computer was hypothetically speaking, never connected to a network. In that case, we would be safe only if the hacker cannot physically access the system. If the hacker is physically able to access the system, he would still be able to enter it using the methods that they typically use.

To demonstrate the point, we'll give you an example of something else that penetrates the system: a virus. The Stuxnet virus was made specifically to target uranium facilities in Iran. While the computers that ran the uranium centrifuges had no active internet connection and were not connected to any outside networks, the virus lay dormant in thousands of devices. Eventually, disaster struck as someone plugged a USB into the system. The dormant virus had affected the USB as well and thus managed to take control of the centrifuges and destroy Iran's uranium and thus nuclear program.

This example shows that the only way to ensure absolute safety is to ensure that the system is never connected to an outside source. With the world now at our fingertips, that definitely doesn't seem to be a viable option!

How does a Hacker Access a Network?

A hacker accesses a network using the steps that we already mentioned in the first chapter. They first find information about the network, then use the information to find vulnerabilities, and then use the vulnerabilities to exploit the system. For clarity purposes, we will give you an example.

Let's assume that there is a server that has 200 active users all logged into the system with access to the files. The hacker would first plan on getting the information on all the users and the system itself. Let's say the system is a website that produces daily content. The hacker would download the site and use a number of tools to analyze who uses the site and what their usernames and emails are.

Once the hacker has that information, he knows that he can now target the users to find a vulnerability in the network. To do this, he might try and crack the password of one of the old unused email accounts that are linked to the site and have access to the files.

After having managed to crack the password (and thus exploited the vulnerability), the hacker would then be into the system and can both get the data or delete it as he wishes. This is why networks are typically very dangerous, and there are a number of security measures employed to ensure that no one can exploit them.

If you have questions over how a hacker can exploit the vulnerability, or how a network is made or can be made secure, then continue reading because we will be digging into the details in the latter half of this book!

Chapter 5: Scripting and Other Tools

Before we dig into the ways that systems can be hacked into in detail, and explain how you can be protected against them, it is important that you know about scripting as well as other tools that hackers typically use. Scripting is one of the main tools in the arsenal of a hacker, and it helps them access the information quicker than they could have otherwise. That makes it important for hackers to be able to script when they are beginning to dig deeper into the world of hacking.

What is Scripting?

Scripting is a way of automating tasks that would otherwise have been had to be written down and coded individually. By running a script, you can basically let the machine do what you would have had to do otherwise. Scripts are typically written in the shell (The black box, so movies didn't get it all wrong!) The help that scripting provides when it comes to hacking is simple. Hackers have to analyze a lot of data to find vulnerabilities or try to exploit them. That would take thousands of lines of code, and mean that cracking into a site would simply not be feasible. With scripts, though, the job becomes way easier. The elite hackers typically make scripts that are used to dig through the system with ease, and with little human input.

What makes Scripts so Dangerous?

What makes scripts so dangerous is how easily available they are. Novice hackers, particularly Script kiddies, typically just use the script to gain access to hacking tools, and can cause DDoS attacks, which can harm companies and cause them thousands in revenue damages. Scripts made to code, or even test, can thus be disastrous in the wrong hands.

Some Script-Based Tools used for Ethical Hacking

Some script-based tools that you can easily find on the internet and use for ethical hacking include:

1) **John the Ripper:** An open-source tool that you can easily download. It is one of the most versatile password hackers and uses intelligent algorithms to decipher passwords based on the encryption of a system

2) **Metaspoilt:** This tool contains a number of scripts pre-written into it that can scan for and find vulnerabilities within any system, and help you exploit them.

3) **IronWasp:** A multiplatform tool that can search for as many as 25 different web vulnerabilities.

With these kinds of scripts being available for public use, the dangers to any small business sites are typically large. That is why it is recommended that you hire an ethical hacker or a programmer to ensure that all such mainstream vulnerabilities are closed off, and the system does not have to suffer as a consequence.

Is Hacking Easy?

Given that we just told you about a number of tools that can help you hack into systems, find vulnerabilities, and crack passwords, you must be wondering if hacking is easy. The answer to the question is somewhat complicated and mostly depends on a few factors.

If you plan to hack a small recently established site that does not use any security protocols and is completely unprotected, then yes, hacking would ultimately be easy. If, however, you're trying to crack the password of another person on Facebook, Jack the Ripper will be of no use to you. To work around those systems, you can't use pre-made widely available scripts since those vulnerabilities would already have been closed off. You would need to observe the code of the system instead, find any potential vulnerabilities, and custom-make a script to exploit it. So in those cases, hacking is definitely not easy, and we can see why ethical hackers are able to bag so much money.

In the later chapters, we will be discussing how hackers attack and how you can stop them from causing damage to you and your system.

Chapter 6: The Different Types of Hacking and How they Work

Now that we know all about the basics of hacking, we will see how hacking actually works by looking into real-world examples and how they work. This will be an extensive list and should let you know about all the major ways that people can hack into your system or account. In the later chapters, we will also consider how you can protect yourself against all of these methods of hacking, and how systems have been made that work to protect you from them.

Physical Hacking

Perhaps the technique of hacking that we get to hear the least about is physical hacking. That is because, in today's world, physical access points are too secure for most people to be able to break through them. Nonetheless, it remains a valid technique for hacking and one that you need to secure yourself against.

Physical hacking involves physically gaining access to the data. This can be done using a number of methods. If you are a data center owner, hackers can typically climb in through the ceiling or through the air vents that are placed for cooling. Unless these places are carefully secured, they can easily grab the data that they require physically.

In cases of a company, hackers can typically masquerade an employee and enter the company, physically hacking into the system and easily being able to intercept and gain access to any data that they wish to.

Another way that a person can physically hack data is by tapping into the lines that connect you to the outside world. While it was much easier to do in the past, and a hacker could have managed to eavesdrop on your phone call had they access to the wire cord, now it has become an increasingly difficult task due to a number of reasons that we will discuss in the later chapters.

Brute Force

While being one of the most common attacks in the past, brute force is no longer used for a lot of websites. Nonetheless, for those that have not secured themselves, it remains a goldmine. A brute force hacking script works in a simple manner. It has a database to go with it that contains any and all possible combinations that could be used as a password on a website. That's trillions of entries!

The brute force command module then begins to enter the passwords one by one into the system. Each time a password is not accepted, it will move on to the next one until it is eventually able to find the correct password. Such an attack obviously takes time to execute, but given the power of computers today, it can be done relatively quickly.

Another innovation in the brute force technology is the usage of smarter scripts. The scripts now don't check every word on the list, but rather check only the passwords that would have been considered valid.

Let's consider that a certain website has the following requirements for the password:

- At least 8 characters in length
- At least one capitalized letter
- At least 1 number
- At least 1 symbol

In such a case, the newer and smarter Brute force script would not start from the typical list, but would rather make a specific list of all possible combinations given the conditions. The first item on the list could thus be @@@@@1aA.

Another improvement has come in the form of how the Brute force attacking module starts to input possible combinations. While initially, it used the list in alphabetical sequence, the program now runs the script to check for common passwords first, greatly shortening the time that it takes for a script to find a password.

Phishing

Phishing is a popular form of hacking, and one of the simplest ones for the hacker. Phishing attacks are now taking more sophisticated forms as well and might be given the name of Smishing.

The basic concept of all these attacks is the same: the person that is trying to hack you pretends to be someone that you trust to get your information out of you. This can be done in a number of ways.

The first method comes in the form of appearing to be a website that they aren't. This is done by naming their website's name closely on the website that you actually wished to visit, i.e., facebo0k.com instead of facebook.com.

The second step comes in the form of getting people to visit the website. They might offer in-app advertising which would offer some promo and people might click it. Once people click on the ad, they are redirected to the fake website that the hacker has made. The URLs are pretty similar, and the website design is exactly the same. The coding is very different, though, and once someone enters the password into the fake website that the hacker has made, the password is saved in a database. Thus while people think that they entered information on a legit website, all the websites would have done would be stealing their data.

The second type of Phishing, popularly called Smishing, refers to the method in which the hacker would try to act as if they're your bank or any other service via email or SMS. It is very easy to spoof your email and make it seem legitimate. This is because the email core does not verify the names of the sender, and people can send an email with whatever email they wish in the sender's name.

So in other words, you could compose an email and put whatever you want in the "Sender" field, if you know how to do so.

The hackers that use this technique usually know some information about you. They might, for example, know what bank you are a customer of. They would then send an email that would have your bank's official email address in the sender field and ask for information such as your card number and pin. That information is then used for fraud.

The third type of phishing is done over the phone and known as Vishing. There are two particular methods that are used in this. The first one involves spoofing the caller ID. This is very similar to email spoofing and allows the hacker to show their phone number as that of a legitimate institution. They use them combined with automated answering machines to steal information.

The second method used is easier if the victim is using a phone line. The hacker calls the victim and tells them of fraud and asks them to call their bank to confirm. They then pretend to hang up, playing flat tunes to indicate that the phone has been hung up. In reality, they're still on the other side of the line. The victim then calls the bank, and the hacker pretends to be the bank and obtains sensitive information that is later used for credit card fraud.

Cookie Theft

One of the more complicated ways of hacking into a system involves cookie theft. This is more complicated than most hacking mechanisms. Cookie theft involves stealing the cookies of a system.

The cookies of a system are authenticating the information that is used to authenticate a person for website usage .

This can be done in a number of ways. Some of the ways include session fixation, Sidejacking, malware, and cross-site scripting. Session fixation refers to when the hacker sets the session to an id that is known to him. He does that by sending a specific link. When the user uses that link to log into a session, the hacker is able to steal the cookies. Sidejacking involves stealing the cookies using the Wi-Fi connection. Many websites do not use SSL certificates on their site, and any data sent can thus be sniffed from the Wi-Fi connection. Cross-site scripting involves tricking the victim's computer into running a script that makes the hacker obtain a copy of the cookies. Malware also digs into a system and retrieves the cookies for them.

Cookie logs the active sessions of a victim. This means that if a victim is signed in to a website, a cookie records that and lets them access the website continuously. Once a hacker has access to the cookie session, they are thus able to validate their own server or system and allow them to log in as well.

Using Wi-Fi for Hacking

While the Wi-Fi offers great accessibility for a user, it is also used as a window to hack into the system or a network. There are a number of ways that this can work. The first one involves a hacker targeting one particular person. They look at their schedules and find a way where they use the internet a lot, for example, at a cafe.

They then set a fake WAP at the Cafe, naming it the same as the WAP that the victim typically uses. Once the victim is connected to their face Wi-Fi access point, they can read all the information that goes through it.

Another way is not to target a specific person but to target all the people in a specific area. So taking the Cafe example again, a hacker would simply set up a Wi-Fi access point in that location and let people connect to it. While people connect to it for free internet, the hacker can then read and access your data that you transmit through your Wi-Fi. This includes sensitive information, including passwords.

Trojan Horse

If you've read the Greek story of the infamous Trojan horse, you already know what you're dealing with here. The Trojans posed the horse as a gift and gave it to the Troy people. It was meant to show that the Trojans had given up, and Troy had won. In reality, though, the Trojan horse housed the army of Greece, which ambushed the city once the horse was pulled inside.

The virus functions in the same manner. It presents itself as software. Typically, Trojans tend to enter your system when you are trying to download software from unauthorized sites. The software isn't actual software and is just pretending to be one. Once you have installed the software, the Trojan can freely roam in your system.

The function of such a virus is to give control to the hacker by installing rootkits.

By installing a Trojan in the system of the victim, the hacker can obtain control of the system of the victim. This means that they can do anything in the system of the victim, including accessing all data and deleting or transferring any data that they wish.

This makes the Trojan horse virus a particularly dangerous one, and antiviruses usually have dedicated functionalities to ensure that no Trojan goes undetected.

Keylogger

In a lot of ways, a keylogger replicates the behavior of a Trojan. It enters the system in a similar manner, but there are differences that we must take into account. The keylogger has a very simple function and is thus typically easier to develop than a Trojan horse. What that means is that most hackers can easily use it by getting someone to download fake software.

The function of a keylogger is to log keystrokes. What that means is that it records all the keystrokes that a person makes on their system. This allows the hacker to access both personal information that a person may have typed out, as well as any passwords that a person inputs in the system. That way, he can easily gain access to the different accounts of the victim and use them for whatever purposes he wishes.

Keyloggers are now also able to carefully analyze the data that is input into them and dig out any passwords for the user, making it way easier to use them. They are thus a simple yet efficient way to hack into a system.

Drive-by Downloads

Drive-by downloads are websites that can force your browser to download a file when you visit them. These are powerful tools if someone is unable to convince other people to download malicious files on their own. Using this technique, the hacker can thus automatically get a file to download on a person's system and leave them vulnerable to Trojans and keyloggers, among other malware.

Social Engineering

One of the more modern and sophisticated techniques of hacking that is now commonly used requires very little technical knowledge. Social engineering is exactly what the name says. It's a method by which the hacker socially engineer their way into your system.

They do this by manipulating people on a human level and attempting to get confidential information out of them. The information that can be received includes things such as parent's names, credit card and other document related information, and other things. Once a person is able to access all of this data, they can steal the identity of the person to hack the system.

They do this by using the information that they have gained to prove that they are the owner of the user ID. Typically, forget password IDs can redirect you to security questions. These include Social Security Numbers and other such information.

With the information that the hacker has now gained, they are easily able to cross the system and reset the password by assuming the identity of the person. This is a lengthy technique and often takes time since it would require the hacker to gain the trust of the victim .

Chapter 7: How to Protect yourself from Hacking

Now that you know the different types of hacking that exist, it would be important to know how to protect yourself from them. Without having adequate protection and without knowing how you can ensure that you remain safe from these kinds of attacks, you would let yourself be very vulnerable to hacking. Let us explore the different ways in which hacking can occur and look into how you can keep yourself safe in case of such an attack.

Physical Hacking

Physical hacking is perhaps the easiest to save yourself from. Physical hacking requires that a person has access to the travel channels of your data or the storage servers. To ensure that that doesn't happen, you can do a number of things. The first would be to ensure that all your data is encrypted, and password protected. Numerous services offer you the services to encrypt your data, which would render it useless even if someone was able to steal them. Newer hard drives are also encryptable and can have passwords put over them to ensure that no one manages to enter them. However, it is important to remember that while encryption offers some form of safety, passwords on laptops, computers, and hard drives are typically not as great security. This is because brute force can be used on such a system, and would allow for a person to quickly dig into the data.

To secure a premise where your data is contained, a number of additional security measures can be taken. The first thing that you can do is to ensure that there are no vulnerabilities within the floor plan of the place where the confidential data is stored. While vents are necessary for heat sinks from the hard drives, they can be made much more secure by ensuring that better material is used for them. Alarms can also be placed inside the vents to alert the security in case someone tries to hack into them.

Similar measures can be taken in office spaces. A manager should ensure that different profiles are made for each of the employees so that the amount of data they are able to access is limited. This ensures that the lower-level employees that are not required to have access to any confidential data can be shut off from it. Managers should also ensure that the area where the computers and hard drives are kept is secure. There should be no unauthorized person in the place where the servers are kept. This can be done via the installation of CCTV and hiring some security.

In case of the absolute requirement of confidentiality, newer hard drives are available where the data can automatically be deleted in case someone tries to force their way into them. This ensures that no one can access your data and would render any and all attacks useless unless the person making the attacks is already aware of what the passwords are.

When it comes to hackers being able to tap into connecting lines between phones, things can get a lot tougher on the part of the company. It is usually not possible for a company to ensure that no one taps into the line.

However, it is important to remember that landlines offer much higher security than the VOIP options. It is thus important to avoid unsafe connections such as VOIP when you are communicating some confidential information to another person. Moreover, the company should ensure that no one knows when they are making any confidential calls. If the times are not known to the hacker, they would naturally find it much harder to find the information they seek. Eavesdropping on lines all day long is very impractical for a hacker.

If you must absolutely use VOIP or other such vulnerable methods, we recommend using a VPN or a virtual private network. While a number of VPNs now offer free limited services, the services for large amounts of usage would cause you some money. However, they can save you from a lot of hassles. A VPN has a number of features that include identity masking as well as encryption. We will discuss these later.

Brute Force

Brute forcing passwords is one of the easiest things that a hacker can do to get access to your information. While there are a number of measures that internet service providers, as well as websites, have done to ensure that no one can brute force their way through the passwords, there are some cautions that you must take as well.

The first and frankly, the most important cautionary measure that you can take is to make your password difficult to guess. Surprisingly, a large number of people fail to do so. Millions of accounts are cracked into every year simply because the passwords that they choose are among a few of the following:

- Password
- Qwerty
- Their names
- Their pet's names
- Their crush's names
- Their favorite celebrities names
- Other similar easy to get information

This allows the hackers to quickly be able to get through the system and find your password.

Another thing that helps with brute force attacks is to have different passwords. To demonstrate how this helps, let us give you an example.

Consider that a hacker manages to find an application that does not require Captcha clearing before entering passwords again. In that case, they would be able to hack through and get your password on that particular application. Most people keep similar passwords on most applications, and hackers are aware of that. If you do the same, the hacker would now also be able to access anything and everything from your internet banking application to your Facebook account.

If you keep different passwords for all applications, though, you would be able to keep your other accounts safe. There are many accounts that allow you to enter the password a limited number of times, and they would thus be safe.

If it is a hassle to remember a large number of difficult passwords, then you can find a number of applications to help you both find strong passwords as well as to keep them safe and allow you to log in on devices that are already approved automatically.

Phishing

Phishing is one of the easiest ways in which a hacker can access your information. It is luckily also the method that you can easily evade with a little common sense and help. To understand how to ensure that no information is given out using phishing, we have to look into each type of phishing individually.

The first type of phishing comes in the form of websites that are made to replicate other websites that you typically use. These are generally very easy to unmask. First off, you need to ensure that any website that you are linked to via an advertisement or a message is legitimate. For that, you can check the certificate of a site. If a website has an HTTP instead of HTTPS at the start, it is typically a high-risk site, and you should be careful navigating over it. You should ideally carefully read the link to ensure that you are on the right site. There are a number of characters that can easily be confused, including the O and 0, and l and I, so you should pay careful attention to those.

If you have any form of doubt about the validity of the site that is asking you for the password, there is a simple procedure.

You can enter an incorrect username and passwords. Phishing sites do not carry out any validation and simply store the information. Thus it would accept any and all username and passwords that you throw at it. That is an obvious indication of a site being made for Phishing.

The second kind of Phishing comes in the form of emails and SMS. These, although seemingly valid, are typically spoofed. Luckily, the procedure to find out if an email is spoofed is not too difficult. All you have to do is click reply to the email. When you are trying to reply to an email, it is going to be sent to the person that sent the email in the first place, and not to the spoofed address that it showed that the email came from. Thus by clicking a reply, you can easily find out who the email that you will be sending is going to and avoid giving out information if it's anyone not trustable.

Another important thing to remember is never to share sensitive information over email. Companies would never ask you to email them your password or any other similar information, so be wary of such requests!

The third type of Phishing comes as the voiced variant. There are two ways in which that occurs. The first method uses call spoofing. It is important to ensure that you never enter your information on calls that require you to enter them. Your banks would never ask for such information from you via call.

The second type is a scam where the caller pretends to hang up. It is best practice to put the phone down and ensure that the power line is cut before moving on to call the bank.

That ensures that you are safe, and the call was actually held up, and no one is on the other side, trying to listen to your confidential information.

With these simple practices, you can ensure that you are never a victim of phishing attacks and are able to keep yourself safe. These steps are very simple and can save you from a lot of hassles!

Cookie Theft

Your cookies are a piece of information that you should never let hacker access. If a hacker can access your cookies, they can be authorized to enter your accounts and do as they will. That is why you have to ensure that they are unable to get to your cookies in any way.

We previously discussed four different methods in which a hacker can access your cookies. We will now look at how you can save yourself from each one of them.

The first method is session fixation and needs you to click a link to open a session with a particular ID. To ensure that you are not led to a session created to steal your cookies, it is important that you do not use the links that are emailed to you from fishy-looking email addresses. Even legit email addresses should be confirmed by clicking a reply, as we have already mentioned before. These measures ensure that you are never at risk of having a fixated session again.

Sidejacking involves stealing cookies via the Wi-Fi network.

That means that both you and the hacker have to be on the same Wi-Fi network. It is thus recommended for you to keep your Wi-Fi password protected. In case of you being in a public place, you should ensure that any websites that you visit are encrypted. When the websites have SSL or TLS certifications, a hacker would be unable to access the information of the session and fail to steal the cookies.

This can be done in a number of ways. Some of the ways include session fixation, sidejacking, malware, and cross-site scripting. Session fixation refers to when the hacker sets the session to an id that is known to him. He does that by sending a specific link. When the user uses that link to log into a session, the hacker is able to steal the cookies. Sidejacking involves stealing the cookies using the Wi-Fi connection. Many websites do not use SSL certificates on their site, and any data sent can thus be sniffed from the Wi-Fi connection. Cross-site scripting involves tricking the victim's computer into running a script that makes the hacker obtain a copy of the cookies. Malware also digs into a system and retrieves the cookies for them. You can use certain applications that force the encryption to ensure that you are always safe.

The third method that we discussed was the installation of malware. Malware cannot enter your system until and unless you allow for your system to download it. You should ensure that you do not download anything from fishy sites and that you have a good antivirus available on your system for your protection.

The last kind of cookie stealing is done by running scripts on the system of the victim.

The scripts again, need to be executed by the victim. Trickery is often used for that purpose. Many websites would offer you scripts that they would claim would activate your windows or give you an adobe license. All the scripts do is steal your cookies and send them to the hacker. To ensure this doesn't happen to you, don't download untrusted software and never run scripts that you find on unreliable sources on the internet. If a script sounds too good to be true, it most probably is!

Wi-Fi-Based Hacking

Wi-Fi-based hacking can be scary. However, it is also very easy to ensure that you don't become a victim in this case. The first type of Wi-Fi-based hacking is where a person is specifically targeted. For that to happen, the hacker would have to chase you physically. That means that you should know that someone has been keeping tabs on you if you're simply a little aware of your surroundings. If you go to the same Cafe to use your internet at all times and find someone always chasing behind you, then you already know that there is something problematic. You can consider changing Cafes or not logging into an active session in their presence.

The second kind of hacking occurs when someone makes their own WAP and gives out free internet to steal data. A number of remedies are available to you in that case. The easiest one is to never log in to any places using the Wi-Fi that you can't trust, as well as to never send out any confidential information using it. However, that is not the best solution since you might need to connect to Wi-Fi for some reason.

Another better resource is available in the form of a VPN. A VPN, aka a virtual private network, ensures that there is another security layer between you and the hacker, and ensures that they are not able to tap into your data.

Trojan Horse

A Trojan horse is pretty similar to any other malware, and the best way to deal with them comes in the form of simple solutions that are applicable to all other such software.

The first way to deal with Trojans comes in the form of precautionary measures. These measures are made to ensure that the Trojan does not enter your system in the first place. These include measures such as ensuring that you never download software from places that you don't trust. Most third party downloading sites are infected with malware and should be avoided at all costs.

The second important thing to note is that you should not download attachments from emails that you do not trust. If someone has emailed you a random file with no explanation, you should avoid it by all means and not download it, for it may contain malware.

If malware has already entered your system, you need to ensure that it is unable to act and take control. It is especially dangerous once it has accessed your BIOS using a rootkit, so immediate action must be taken. For that, you should, first of all, ensure that you are already using a reputable antivirus. Antiviruses typically already have lists of known Trojans and can easily locate as well as quarantine them.

Another important tool is a sandbox. In case of having to download something that you do not trust, it is recommended that you do so in the sandbox. A sandbox is a virtual container within your system in which you can download any files and test them. If they display abnormal behavior, only the sandbox would be infected and can be deleted. If they are safe, you can then download them directly to your system.

If you are already infected by a Trojan, you should download an anti-malware software such as Malwarebytes to ensure that you can remove it from your system. If the malware has dug into your BIOS as well, you should always perform a BIOS reset to ensure that any rootkits are removed from your system completely.

Keylogger

A keylogger can be a lethal hacking tool. Fortunately, it has its own downs. Any keylogger must be able to transmit data back to the hacker for it to work. That means that there is a strong chance that any firewall would detect the keylogger at work and alert you about it. It is thus important to ensure that your firewall is on at all times to prevent keylogger-based attacks on your system.

A keylogger typically behaves like malware, so the same precautions as a trojan horse apply. You shouldn't download malicious and unknown content, and you should keep your system protected by using a strong antivirus.

For both keyloggers and trojans, one thing that would help is to update your system constantly.

With system updates, you will usually find many of the older exploits are closed down, and the defense is much better, ensuring that your system is kept safe from prying eyes of the hacker.

Drive-by Downloads

Drive-by downloads enable the downloading of malware into your system. There are a number of ways in which you can prevent that from happening.

The first thing that you should consider is to disable auto-downloading options. Most browsers are equipped with an optional turning off of automatic downloads. Any download requests thrown by the website would thus not be processed, and anything that you don't download won't be downloaded.

It is also important to not click links you are sent by a third party or ad sources unless you trust them. The links might often redirect to sites that are made to force downloads of malware.

Having a decent defense system, including a strong antivirus as well as a firewall, can also help. These would immediately quarantine any threat even if it were to be downloaded. It is also helpful to remember that most applications require permission before running. If anything is downloaded automatically, delete it instead of running the script!

Social Engineering

Social engineering is a tricky hacking technique. It is consequently also tricky to avoid. Luckily, with a few precautions, you can generally ensure that you are not a victim of social engineering.

The first thing that you have to remember when it comes to social engineering is to keep your security question and answer safe. Make the answer unique and never tell anyone what it is. Questions like "What's your mother's name" are too easily guessable and should either be avoided completely or should have unique and untrue answers so that no one can engineer their way into your system.

If a sketchy person seems to be taking an unusual interest in particular information that can directly be connected to your bank account, it is usually presumable that the person has malicious intent. You should ensure that no answers are given to such a person, and your personal information remains safe and personal.

Many websites now allow you to set up two-factor authentication and other methods of accessing your information to ensure that you are not made a target of social engineering. You should always enable any such options for added security. It is also usually helpful to have a valid phone number or email address where password reset links can be set. If those exist, most sites will not rely on having to second-guess your identity, potentially letting someone steal it along the way.

You should also ensure that you are aware of the security protocols of your bank. You can normally set limits, transactions above, which would be confirmed from you via the number you provided to the bank. This ensures that no one can pretend to be you and rob you of your money.

Chapter 8: Cybersecurity and How it Saves you from being Hacked

Now that we have gone over some of the basics of hacking and how to prevent yourself from them, it is important to see how systems, as well as websites and applications, aim to save both you and them from hacking. To dig deeper into that information, we have to look at the different ways in which cybersecurity works.

What is Cybersecurity?

Cybersecurity refers to the practice that is used to protect programs, networks, and users from digital or cyber-attacks. They can operate in a number of ways, but the end goal remains the same: to keep the data safe and secure and to ensure that no one can malign, steal, or otherwise destroy it.

We will now explore the different countermeasures that are available against a cyber-attack and how they can help a network evade any form of attack.

Countermeasures by Design

Countermeasures are designed to mean that a system is made to ensure that the maximum amount of security is available to the network and its users. The design elements that can help with security offer a number of features.

One of the main design features to ensure high security is the principle of least privilege.

This is a very simple mechanism and offers any user only the minimum authority within a system, as is needed by them. This ensures that even if a hacker assumes the role of anyone within a network, they would be unable to do much and would not be able to access data, alter it, or delete it .

Other design mechanisms that can enhance security include defense in depth. This refers to systems where you need to breach more than one aspect of the system to be able to penetrate it. So, for example, a system might need authorization from both user 1 and user 2 to allow access to anyone to the sensitive data. This design means that the hacker has to hack through multiple security systems, and makes it much harder for a hacker to be able to gain control.

Another important design measure comes in the form of audit trails, which ensures that if any vulnerability is detected, either through black hat hacking attacks or otherwise, it is promptly dealt with, and the system is not left vulnerable in the end. This keeps the system safe from further attacks down the line.

Security Architecture

This form of countermeasure aims to design the system in a way that makes hacking difficult. This is mostly a design-based system but rather deals with how various entities within a network interact with each other. By limiting the dependence of a system on other systems, we can ensure that the hacker does not gain control of the whole system even if he enters a part of it.

Another important role of security architecture is to ensure that any and all entries and vulnerabilities are covered by the security systems in place. It thus dictates where the security measures are placed to ensure that no vulnerabilities remain.

System Penetration Testing

An important way of checking the security design, architecture, and strength of your system is to do a system penetration testing. A penetration testing, which is also popularly known as pen testing is a way of accessing the vulnerabilities within a system to ensure that all of them are closed. There are a number of ways in which a system can conduct penetration testing to ensure that there are no vulnerabilities within the system

If a company, system, or network does not have the resources to hire themselves a hacker, they can usually use software that is already available to conduct such tests. These include tools like MetaSpoilt that we have already discussed. These tools have distinct functions. When they are made to test a network, they will find out all the vulnerabilities. Many tools also exist that can both exploit these vulnerabilities to assess the damage to the system that would occur in case of an attack, as well as provide solutions to these damages to ensure that they do not occur in the future.

For the best service, though, the automated tools are left far behind. The persons that one should refer to for the best analysis are the white hat hackers.

White hat hackers are usually skilled in penetrating a system and can quickly point out flaws that would not have been pointed out by any other traditional script. However, they can be expensive to hire.

When a white hat hacker is hired, you can make them test the system in two ways. The first type is black box hacking and would mean that the hacker is not told any facts about the network. This is a useful method if you also wish to see how easy it is to find information about your network. Having accessed the information, the hacker would then write scripts to find vulnerabilities, in a much more efficient way than the pre-written scripts could have done. These vulnerabilities are then reported back to the person that hired the white hat hacker to ensure that they can be closed. Black box testing is a good way to see the practical security level that your system holds.

Another type of white hat hacking can be employed. This type revolves around a white box methodology. What that means is that the hacker is already told all the information that he needs to know about the network, and the code and system are transparent before him. This is especially beneficial when you want an in-depth penetration testing since, with the information that the hacker would already have, he can dig much deeper into the vulnerabilities. Most companies would use a mixture of white box and black box based white hat hacking to ensure that the hacker is both able to find the issues in-depth and able to show a realistic strength value of the system.

Elite groups of hackers are usually able to write scripts that other hackers cannot hope to reproduce. They are thus typically paid way higher, and companies tend to employee them to find any flaws where the business model requires high network security. Such models can include government websites as well as websites of cloud storage apps.

If cost is an issue to you and you feel that your system is already impenetrable, a new form of white hat hacking contracts is now becoming popular. These are performance-based. A forum of hackers is offered a bounty for being able to hack into the system of the company. If no hacker succeeds, you already know your system is strong enough. If someone does, you need to spend the money only in that case. This helps save money if you're already sure of your security.

Two-Factor Authentication

One of the prime ways to ensure that no one is easily able to access the system is to use two-factor authentication. That means that you need two distinct pieces of information to access the data. These typically include one pin or password, and one hardware or biological trait. Typical systems can combine pins with thumbprint scans. Having a system that is based on these traits can mean that it is much more secure. Fingerprints are hard to replicate and typically require access to the victim. Similarly, for any cards using NFC to allow access to a system, the victim's card must be stolen. In such a case, a victim can usually quickly inform the system about a stolen card and thus ensure that the system is not compromised using it.

Having a two-factor authentication can thus make your system much more secure, and make penetration much more difficult.

Data Security: Encryption, Protocols, Packets, and Transmission

Data has to travel around a lot. That leaves data very vulnerable. If data is sent through a simple wire with nothing to hide it, hackers can simply dig right into it. That is where the data security features come in. There are a number of ways in which data is protected. We will explore each of them in detail to see how your data manages to travel from one place to another safely.

If your data is traveling in the form of simple radio waves or through copper lines, anyone with the right software can read the data and thus be able to get your information. Radio waves are particularly unsafe since you don't need to find a line to tap into physically, and the risk of being caught is thus mitigated. Newer technologies now rely on fiber optics, which is more secure. This is because when someone tries to tap into a fiber optic, it will break the glass and possibly trigger alarms. This means that data that travels through that channel is typically much more secure.

However, most of the systems, especially WAN and remote areas, continue to use radio waves or copper-based wires. Fiber optic is also not impenetrable in any way. That is why data transmission is risky.

To help mitigate the risk, a number of ways are used. These include encryption and packet-based transmissions. We will look into both of them in detail.

Encryption means that data is distorted so that it is not readable. The earliest forms of encryption include the easier Caesar cipher, more popularly known as the shift cipher. The protocol is basically simple. The data in such a cipher is simply encrypted by using a shift. Thus a is transmitted as b, b is transmitted as c, and so on so forth. Of course, given the computing power of today's world, such algorithms are obsolete. We now have more reliable solutions to ensure our security.

There are two basic types of encryption. The first type is symmetric encryption. Data that has been encrypted using this form of encryption can only be decrypted by using the same key that encrypted it. This means that the key has to be transferred as well. This can lead to a security risk since hackers can ultimately intercept the key as well. However, if the key is transmitted in a secure manner, no significant concerns should arise.

Data is typically transmitted as packets. This means that not all the data is channeled at once, but data is rather divided up into small packets that are sent simultaneously or one by one, through a network. All of these packets then combine at the end receiver to make a complete data set, which can be decrypted using the key that was transported by any means. If you are using symmetric encryption, it is thus very important to ensure that the key is kept safe.

In using asymmetric encryption, the data is encrypted using a public key and decrypted using an individual private key. Since the key does not have to be shared, it is typically thought to be more secure. Nonetheless, you have to keep the key safe and ensure that no one can assume your identity or steal your cookies for that to work. Websites that use asymmetric methods of data encryptions typically have the HTTPS tag and have SSL technology, which ensures that any information that you enter on those sites is kept secure. You shouldn't enter sensitive information on websites that lack those protocols.

There are various algorithms that are used within encryptions that are important to know if you wish to keep your data safe. The earlier algorithms include the DES and triple-DES that were found to eventually become vulnerable as technology caught on and was able to brute force the algorithms. Newer algorithms such as the AES can make your data virtually unhackable. Using the current technology, AES 256 encryption would take billions of years to crack!

Protocols define how the algorithms should be utilized, and allow for secure key exchange among other functions. The protocols are thus an important part of the process since they allow for the data to be readable to the intended user.

So to summarize, while data can still be tapped into, it is often kept in the form of cryptic algorithms that can only be decrypted using keys that are transferred using secure protocols such as SSL.

As long as a system sticks to the protocols, encrypts the data, and uses protocols like SSL to keep their data secure, the system itself cannot be brute-forced, and that means that vulnerabilities in terms of data in transit are minimalized.

Encryption is also possible on data at a resting stage, and with those, you can similarly ensure that the data cannot be accessed. However, the decryption keys are usually kept behind simple passwords that can be brute-forced. To ensure that brute force attacks do not succeed, a network can use a number of smart security designing that we will next explore.

Preventing Brute Force Attacks

Brute force attacks can both be used to hack into a system that stores data at rest, as well as to access the data of the users of the network by finding their passwords. With there being a very limited selection of passwords that people typically opt for, and computing being super powerful now, it is hard to prevent an attack that focuses on brute force. Luckily, with a few changes in design, this can be rendered useless.

The important thing to remember here is that a brute force attack aims to mainly get access to the data by having an infinite number of tries at guessing the password. Systems have now been designed to restrict the number of tries that a person can have at guessing. Most online log-in applications would either send ReCaptcha tests that the brute force algorithm would be unable to solve and thus stop it, or would simply lock the account down after a number of tries. Doing this, they are able to ensure that the brute force mechanism cannot continue to dig into the system.

This is an important aspect of security since by adding this feature, you can ensure that even if someone manages to reach your key and has to guess a password simply, they would be unable to do so quickly .

To make things even more secure, logs can be taken of attempts at logging in to a system. The logs will show when someone tried to log into a system and the passwords that were input. This means that the admin can be altered about a brute force attack, and measures can be taken to ensure that care is taken of it.

By using this measure, a network can ensure that no one is able to gain unauthorized access by way of guessing passwords. It is also a helpful feature to include in case of a website having web portals, and many applications such as Gmail and Dell do make extensive use of it to ensure that the accounts of individuals registered for their services are not compromised.

Firewall

A firewall is an underrated aspect of network security. In simple terms, a firewall monitors all incoming as well as outgoing traffic and governs it via specified rules. This is very important since otherwise, people can simply send packets of malware to your system.

A firewall is a wall between your network and the outside world. It inspects all incoming data packets and reads the protocols, including FTP, HTTP, and DNS.

It then uses the rules that are predetermined to decide if a packet should be allowed into the system or not. Similarly, it also inspects packets going out of the system. This is useful since, in case of a hacker using scripts to gain data or logging your keystrokes and trying to access them, the firewall can inspect the packets and identify there being something wrong, and thus block transmissions.

Given the function of a firewall, it is absolutely crucial for a system to have a good firewall. Firewalls now come with greater functionalities, and features and customizations are pretty simple and straightforward. Companies that require the ultimate security solutions could customize a firewall to their needs and ensure that no data is transmitted in or out of the system without proper authorization.

A firewall is the first defense that a system has, and can be useful by preventing malware from getting into the system and preventing system data from flowing out. A strong firewall is thus protection we should all consider getting.

Anti-Virus and Anti-Malware Software

Anti-virus and anti-malware software typically form a secondary line of defense. The function is simple. They scan the system and try and find any programs that are known for being problematic. Most anti-viruses have huge repositories of codes and can easily identify viruses and trojans by matching them with the codes of other known threats.

The threats are then alerted to the system admin, who can then decide to quarantine or remove the threat. Such removal ensures that the threat is no longer active. They can identify a number of threats, including trojans, rootkits, spam and scams, phishing, and DDoS.

Given the versatility of this software, it is absolutely essential for anyone that works with sensitive data to get one of the premium plans of a reputable anti-virus. By doing so, not only would they be able to identify any trojans or other malware, but they would also be kept safe from phishing attacks and other such hacking methods.

Internet of Things: The Unpatched Cybersecurity Threat

One of the prime things that can cause a system threat is via the internet of things. The internet of things refers to any and all things that require internet or network access to work. These include a number of things, including modern homes, garage doors, cars, printers, refrigerators, and whatnot. With a large number of manufacturers now letting you control your electronics using your cell phone, the internet of things becomes all the more important.

Sadly, we see that vendors typically give very little emphasis to this industry in terms of cybersecurity, and simple patches that would seal vulnerabilities are never made. This means that everything from your printer to your garage door is hackable and can be hacked with ease.

Given the digital world that we are moving to, it is high time for manufacturers to place more emphasis on the security of such systems and to ensure that they are made as secure as the other systems are. Ultimately, all networks should be made secure so that hackers can no longer be a menace, and without a focus on the internet of things, we can expect to continue to see successful cyber-attacks.

How are Cybersecurity Tools used to Secure your Wi-Fi Connection?

Wi-Fi connections are typically very vulnerable. If you are going to be using a public router, in a hacker's eye, you're an easy target. Luckily, with newer system updates, many operating systems include inbuilt protection against such attacks.

Taking the example of windows, when you connect to a network, a system will typically ask you if the network is public or private. In case of you being on a public network, windows will automatically hide your device and make it undiscoverable. This ensures that you are kept safe, even where you are connected to a public network. It is important to be still wary, though, since the network admin can still see the information that you transmit, and WAP attacks are commonplace. That is where a VPN comes in. Let's explore a VPN in more detail.

Virtual Private Network

A VPN or a virtual private network allows you to transmit data using a public network as if you were transmitting it using a private network. There are a number of ways that this is achieved, and we will look into some of them.

To start with, a VPN masks your identity and shows a different IP address. This is typically done by masking your IP with another IP that belongs to the VPN server. This means that anyone that intercepts the data will not know where the data came from, and would rather believe it to have come from a virtual IP address that the VPN sets for you.

Secondly, VPN tunnels past the public servers. This means that the data that is sent through the VPN is delivered through packets. Each of those packets has a protocol and is duly encrypted. The encrypted packets cannot be decrypted in the public network, and would only allow the intended recipient with the key to decrypt them. Thus even where the WAP hacker manages to get a hold of the packages, he would be able to find little use for them. VPN thus ensures that you get the maximum security, and your data is kept safe. It is very important for a firm to use VPNs if they are transmitting highly sensitive data over Wi-Fi since Wi-Fi can be hacked into and allow for someone to sniff the data. That is why VPN, along with other cybersecurity methodologies, becomes an important part of any defense arsenal against cyber-attacks.

Conclusion

Now that we have analyzed all the ways that hacking occurs and the tools that hackers may use to enter a system, as well as mentioned the ways in which you can ensure that you remain safe from hacking, we hope that you have found the answers to all the burning questions that you had.

A few short takeaways include that your data is very vulnerable, and everyone, even newbies, can crack into it unless you take steps to secure it. This is especially true for networks since more people tend to want to break into networks. That is why one should always ensure that their network is able to past the penetration tests and has an adequate design. This would ensure that the data of both the network and the customers are kept safe.

There are a large number of ways in which you can protect yourself, and the best combination for you depends on your individual needs. A website that uses no Wi-Fi-based communication networks in public, for example, would not need a VPN tunneling based security system. Similarly, any network that blocks out all external data and takes no inputs would have no use of a firewall.

Whatever your business model or product may be, irrespective of if you're a simple social media user, a small company, or a large network, hacking is a menace to anyone connected to the internet. That doesn't mean that it has to be that way.

Hacking can be fought against in simple steps that we highlighted in this book, and by using them, you can ensure that your data and identity are never compromised again.

Remember, prevention is better than cure. Once a hacker has your data, it is really hard to be able to retrieve it and get it deleted from the internet. You should thus ensure that you follow the guidelines that are made to ensure that your accounts do not get hacked, and you should ensure that your network has a proper cybersecurity plan that it uses to protect itself against any such attacks. We hope that this book was helpful to you in achieving your ultimate hacker-free dreams and that you will now surf the internet safer (or make a career out of ethical hacking!)