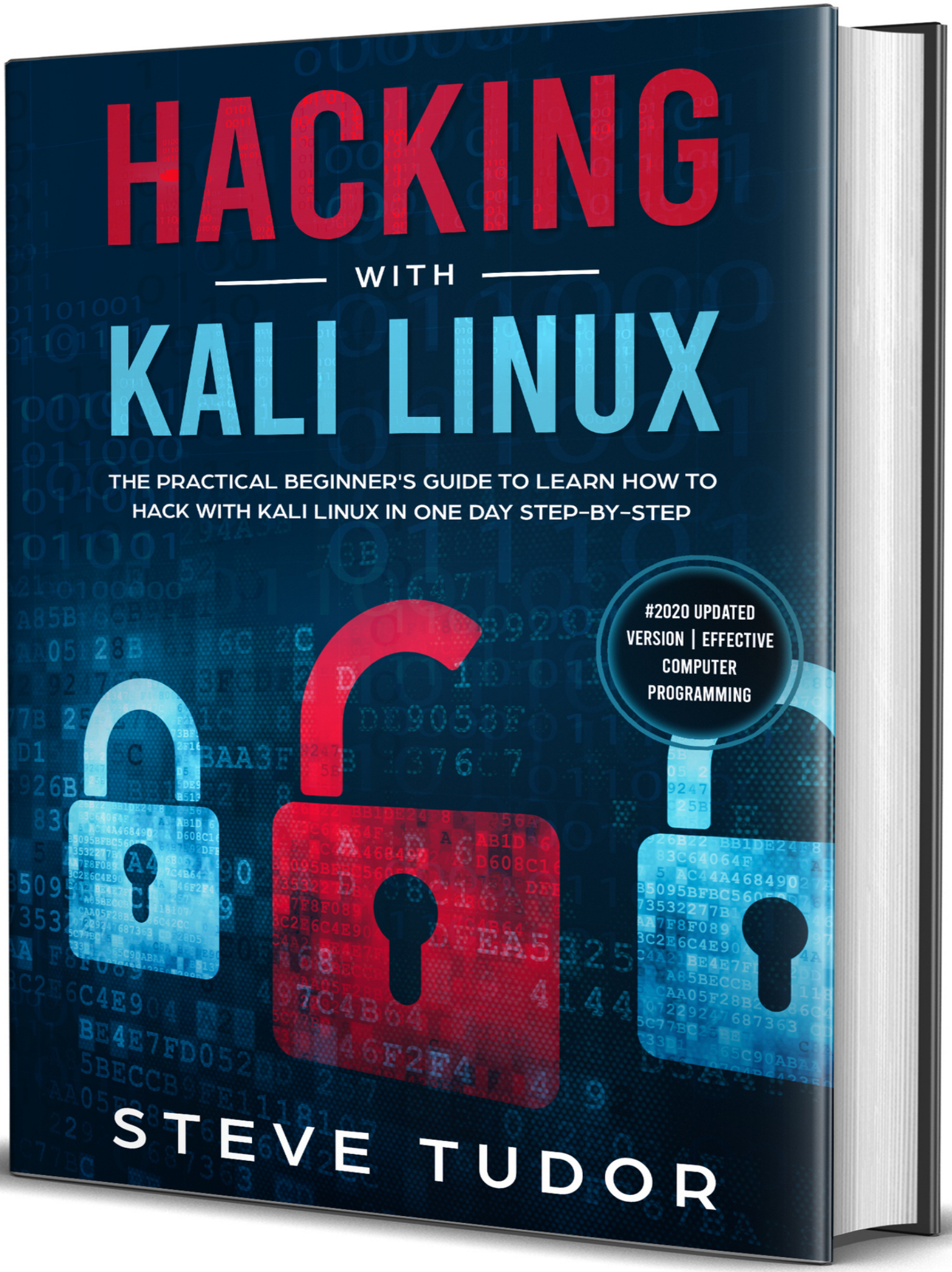
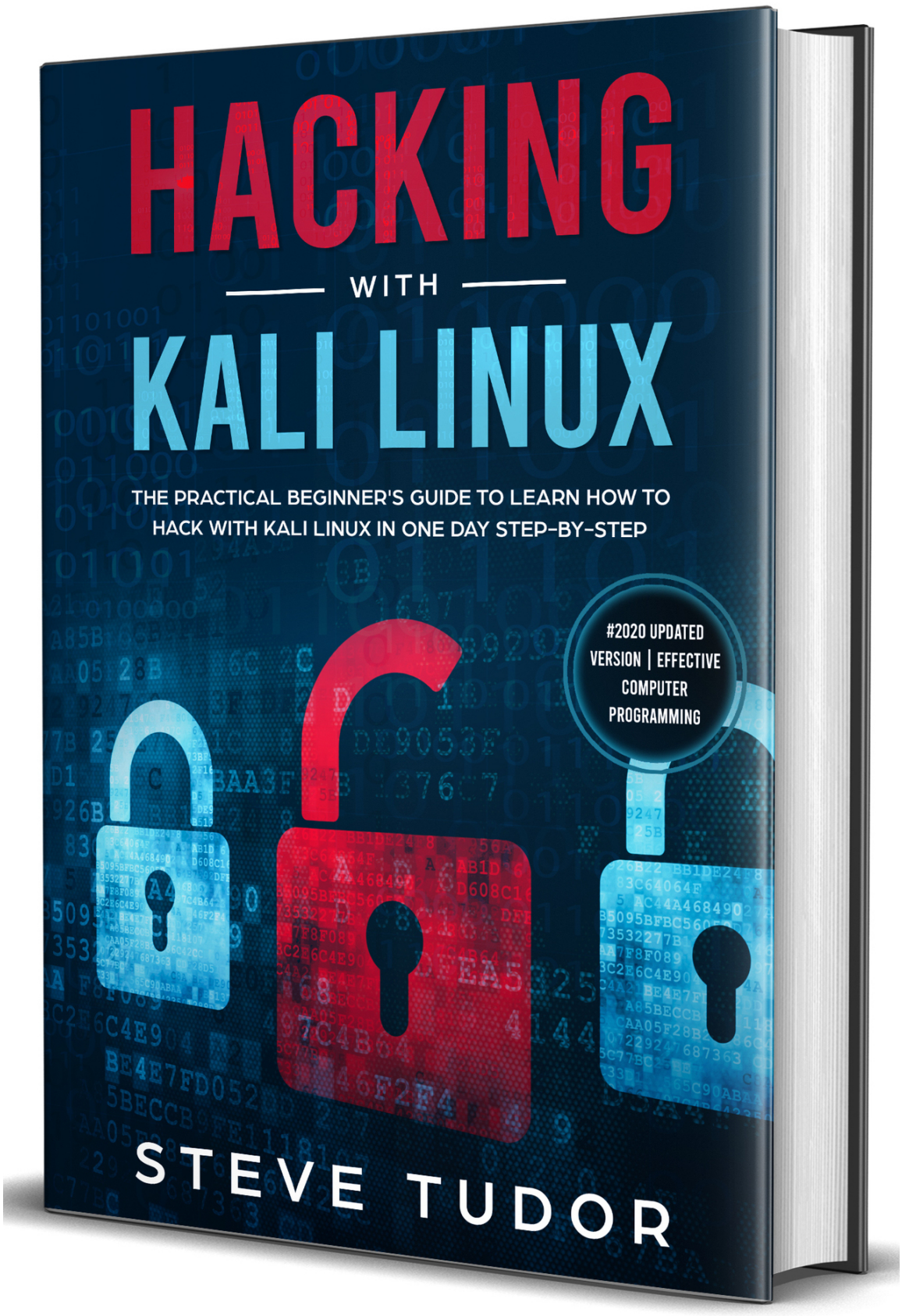

HACKING
WITH
KALI LINUX
THE PRACTICAL BEGINNER'S GUIDE TO LEARN HOW TO HACK WITH KALI LINUX IN ONE DAY STEP-BY-STEP
#2020 UPDATED VERSION | EFFECTIVE COMPUTER PROGRAMMING
STEVE TUDOR


HACKING
WITH
KALI LINUX
THE PRACTICAL BEGINNER'S GUIDE TO LEARN HOW TO HACK WITH KALI LINUX IN ONE DAY STEP-BY-STEP
#2020 UPDATED VERSION | EFFECTIVE COMPUTER PROGRAMMING
STEVE TUDOR

HACKING WITH KALI LINUX

The Practical Beginner's Guide to Learn How To Hack With Kali Linux in One Day Step-by-Step (#2020 Updated Version | Effective Computer Programming)

Steve Tudor

Legal & Disclaimer

The information contained in this book and its contents is not designed to replace or take the place of any form of medical or professional advice; and is not meant to replace the need for independent medical, financial, legal or other professional advice or services, as may be required. The content and information in this book has been provided for educational and entertainment purposes only.

The content and information contained in this book has been compiled from sources deemed reliable, and it is accurate to the best of the Author's knowledge, information and belief. However, the Author cannot guarantee its accuracy and validity and cannot be held liable for any errors and/or omissions. Further, changes are periodically made to this book as and when needed. Where appropriate and/or necessary, you must consult a professional (including but not limited to your doctor, attorney, financial advisor or such other professional advisor) before using any of the suggested remedies, techniques, or information in this book.

Upon using the contents and information contained in this book, you agree to hold harmless the Author from and against any damages, costs, and expenses, including any legal fees potentially resulting from the application of any of the information provided by this book. This disclaimer applies to any loss, damages or injury caused by the use and application, whether directly or indirectly, of any advice or information presented, whether for breach of contract, tort, negligence, personal injury, criminal intent, or under any other cause of action.

You agree to accept all risks of using the information presented inside this book.

You agree that by continuing to read this book, where appropriate and/or necessary, you shall consult a professional (including but not limited to your doctor, attorney, or financial advisor or such other advisor as needed)

before using any of the suggested remedies, techniques, or information in this book.

Table of Contents

INTRODUCTION

The comprehensive offensive and defensive security suite included in BackTrack Linux made it the tool of choice for hobbyists, security professionals, legitimate penetration testers, and black hat hackers alike. The developer of BackTrack, Offensive Security, eventually rewrote the distribution, renaming the project as **Kali** Linux. Kali installation packages and virtual machine images are available free of charge. Offensive Security also offers for-pay courses in security using Kali, as well as professional certifications and an online penetration testing environment.

KALI TOOLS

The centerpiece of Kali Linux, and the primary reason for its popularity among hackers and security professionals, is its extensive and well-organized suite of free tools. Kali currently features over 300 tools including passive information gathering, vulnerability assessment, forensics, password cracking, network analysis, wireless hacking, and a powerful set of exploitation tools. Although all of the tools included with Kali are free and open source and can be downloaded and built onto most (Debian-based) Linux derivatives - having a tested, vetted OS that comes native with such a large array of tools is an invaluable resource.

Among the most useful tools that come with Kali are:

Metasploit Framework – Metasploit is a popular vulnerability exploitation platform containing various analysis and penetration tools. It features multiple options for user interface and provides the user with the ability to attack nearly any operating system. Kali also contains **Armitage** , a graphical management platform that helps the user organize the operations and interactions between multiple Metasploit tools during an attack.

Wireshark – Wireshark is a multi-platform real-time network traffic analysis tool. All traffic on a chosen network node is captured and broken down into useful packet metadata, including header, routing information, and payload. Wireshark can be used to detect and analyze network security events and to troubleshoot network failures.

John the Ripper – John the Ripper is a legendary password cracking tool containing multiple password attack algorithms. Although originally written exclusively for Unix, John the Ripper is now available on several OS platforms. One of its most useful features is its ability to automatically detect the password encryption "**hash** " type. The free version of John the Ripper available on Kali supports the cracking of many password hash algorithms, but not as many as its commercial counterpart.

Nmap – Nmap, short for network map or network mapper, is a common hacking tool that is essential for penetration testing. Nmap allows the user to scan a network for all connected hosts and network services, providing a detailed view of the network's structure and members. Additionally, Nmap provides a list of each host's installed operating system as well as its open ports. This allows the user to zero in on known vulnerabilities during exploitation.

Aircrack-ng - Aircrack-ng is the quintessential software package for wireless analysis and penetration testing, focusing on Wired Equivalent Privacy (**WEP**), Wi-Fi Protected Access (**WPA**) and **WPA2-PSK** Wi-Fi encryption protocols. This tool features wireless packet sniffing, packet injection, wireless network analysis, and encrypted password cracking tools. Aircrack-ng requires network interface hardware that supports **monitor mode** functionality. Kali also features a more graphically-based wireless hacking tool known as **Fern** .

BurpSuite – BurpSuite is a collection of tools that focus on the exploitation of web applications. These programs interact to not only test applications for vulnerabilities, but also to launch attacks.

The list above is by no means a complete one, but it is a representative sample of the power and flexibility that Kali Linux provides as a platform for penetration testing and for computer security in general. Kali can be run live from optical or USB media, as a standalone OS on a desktop or laptop workstation, as an alternative in a multiboot system, or within a virtual machine inside another host OS.

CHAPTER 1) HACKERS

In the most elemental definition, hacking can be described as the act of exploiting the weaknesses and shortfalls in a computer system, as well as the network of such a system. In the exploitation of these weaknesses, illegal acts might include stealing private information, accessing a network's configuration and altering it, sabotaging the structural view of the computer's operating system and much more.

Hacking is practiced in almost all countries. However, it predominates in developed countries. The advancement of information and technology within the last two decades has shown that most hackers are based in developing countries such as in South Asia and Southeast Asia.

The term "hacker" is the source of a lot of controversy today and is confusing to many people. Some regard a "hacker" as someone who has the power to make a computer do anything at will. In another context, a hacker is viewed as a computer security specialist whose primary job is to find the loopholes in a computer system or network and fix them. These loophole finders are sometimes referred to as crackers. All of these ambiguities in the world of hacking have made it hard to identify who a hacker is, a fact that also makes it extremely difficult to detect the activity of a hacker who may be playing around with your system.

A plethora of reasons are behind hacking. Some people are into hacking simply to make money. They can steal your password, break into your private information or even alter your correct information and make it incorrect all for monetary gain. Other hackers are in the game just for a challenge or competition. Furthermore, some hackers are the computer world's equivalent of social miscreants, whose purpose is to gain access to a network or system. After gaining access, these hackers will render the network useless so that the users cannot use it properly.

For example, if a community is protesting against something, it can try to hack into a system as a sign of protest against the authorities. It can choose to do this instead of breaking other laws that it considers to be important.

There are different types of hackers who have various intentions. Based on their modus operandi, we can classify hackers into the following:

1. WHITE HAT HACKERS

These are the good guys because they do not have evil intentions. Perhaps they are named “white-hat” hackers because the color white signifies purity and cleanliness. They hack into a system to eliminate its vulnerabilities or as a means of carrying out research for companies or schools that focus on computer security. They are also known as ethical hackers. They perform penetration testing and assess the vulnerabilities of computer systems.

2. BLACK HAT HACKERS

Black hat hackers hack with a malicious intention of breaking every rule in the book. They hack for personal gain, as well as for monetary reasons. They are known to be from illegal communities that perfectly fit the stereotype of computer criminals. Black hat hackers use a network’s weak spots to render the system useless. These hackers will also destroy your data and information if they are given the chance to do so. When these hackers get into your system, they will threaten to expose your private information to the public with the goal of getting you to do whatever they want. Needless to say, black hat hackers will not fix vulnerabilities in your computer system or network, but will use them against you.

3. GREY HAT HACKERS

The intentions of grey hat hackers cannot be compared to those of the hackers mentioned earlier. These hackers will trawl the internet and look for weaknesses in a computer system or network and hack into it. They may do this to show loopholes in the network to the network administrator and suggest ways of rectifying those loopholes for a given price.

4. BLUE HAT HACKERS

It is said that the color blue represents a member of law enforcement, although this is just a convention. These hackers are freelancers who sell their hacking skills as a service. Computer security firms hire hacking experts to test their networks so that they can be checked for weaknesses, vulnerabilities and loopholes before they are released to the public. Blue

hat hackers are “good guys” and are different from grey hat hackers, whose intentions may be unpredictable.

CHAPTER 2) THE PROCESS OF HACKING

A. HOW THE PROCESS OF HACKING WORKS AND HOW ATTACKERS COVER THEIR TRACES

A computer, as a standalone piece of hardware, is not an intelligent machine. It is the programs written for the computer that determine what it can and cannot do. This chapter will teach you some of the basic principles of programming, as well as how to choose a programming language. At the end of the chapter, you will find an exercise that will help you write a program in Python computer language.

Why You Need to Learn a Programming Language to Hack

Computers operate using a series of switches. These electronic switches are turned on/off in different combinations. This creates the functions of a computer. For a computer to turn a switch on or off, a computer program sends a message using binary code. Binary code is a series of 0's and 1's, with the 0's meaning on and the 1's meaning off.

The problem with binary code is that it is incredibly complex. It would take even advanced programmers a long time to interpret the code, let alone alter it to do what they want. This is where a programming language comes in.

A programming compiler translates pre-determined commands from the programming language into binary code that can be read by the computer.

A Few Considerations (and Key Terms) Concerning Programming Languages

To choose the best program to learn, you should consider what you want to do with your hacking/computer knowledge. Here are some common terms you may come across as you learn about the different programming languages:

Language Generation

Generally speaking, as technology has advanced, so have computer languages. Currently, there are five generations of computer language-

- First generation (1GL) were the most primitive. They were difficult to write, since it was written in binary code (0's and 1's).

- Second generation (2GL) are often referred to as assembly languages. It was the first step that allowed programmers to use symbolic names for commands, rather than just binary code.

- Third generation (3GL) was another advancement, with higher level languages like Javascript, Java, C, and C++ being developed. 3GL allowed commands and words to be used in programming.

- Fourth generation (4GL) is a type of coding similar to human language. This programming is common for database access, with some of the most common being ColdFusion and SQL.

- Fifth generation (5GL) is the most advanced language by far, with its applications for neural networks. Neural networks imitate the inner workings of the human mind and are applied in the area of artificial intelligence.

B. RECONNAISSANCE IN ACTION

One of the most important things that Hackers do when they decide to attack a system (server, network, etc.) is to gather as much data as possible about it.

Think in the following way: when you want to go for a holiday in a place / country where you have not been, what are you doing? Most likely, you do homework. You mean you're interested in that location. You are looking for different things on Google (what you can do there, such as weather / food, reviews of places in the area, etc.). In other words, you **inform yourself about your target** .

Exactly through this process a hacker passes when he decides to attack a system. There are different ways you can learn more about a site / server, one of the simplest methods is to search Google for information about it.

With a simple command like **nslookup** (or **dig**), you can find out with the IP address of a site, and with the whois command you can find out more about that domain.

> **nslookup** google.com
> **whois** google.com

The term Reconnaissance (or Information Gathering) comes from the idea of researching, informing you about a particular topic before moving on to action. In short, basically it means **documenting** before the **action** .

As a matter of time this process is most "expensive". Why? Because an attacker needs to be very well informed, he needs to know things in detail because otherwise (as we said in step # 5) risk his own freedom.

C. SCANNING THE SYSTEM

The next step in the "Hacking Process" is **scanning** . Once a Hacker has more information about his target, he will begin to learn more (technically this time). And how will he do that? Using a variety of tools (such as Nmap) to scan networks, servers, and provide clearer information about network topology, used equipment, operating system, and more.

Why are they important? Why is it important for a Hacker to know if a particular web server is running on Windows or Linux? Because once it has this information it can go further (step 3) with a little research on Google to discover some existing vulnerabilities and try to take advantage of them in order to gain access to that system (or to extract certain data).

D. GAINING ACCESS TO THE SYSTEM

Having done the themes (done research, scanned networks / servers, learned information from different sources - Google, Facebook, Forums - about the target), the hacker can start the attack. The attack should be very well thought to be in stealth mode (without triggering alarms and - if possible - without generating too many logs).

There are a lot of **tools** (**Burp Suite, SQLmap, Metasploit,** etc.) that can be used to generate a cyber attack, everything depends on technology and objective.

Getting access can be done in several ways and from several points of view:

- **Getting** root **access on a Linux server**
- **Obtain access to a** site's **administration** panel
- **Obtaining** access **to a particular** network **equipment (Router, Firewall, Switch etc.)**
- **Get** access **to a network's** end device **(smart phone, tablet, laptop, etc.)**

Once the hacker has access to one of the items listed earlier, he is infiltrated into the network and can get a lot of information about the organization he is (digital).

E. MAINTAINING ACCESS

Once in the network, Hacker has the option of retaining access. In many situations when different servers of major companies (Yahoo, Google, Microsoft, etc.) have been broken, Hackers have always left open doors to get back into the system.

These wickets are called "**backdoor** " and are intentionally left by Hackers (or even by the software developers of any applications that you and I use day by day) to have access later in the system.

So they can constantly extract data, track what's happening in organizations, hold back control, and then do something with these data (usually they are sold on the black market on the Deep Web).

F. COVERING TRACKS

This is a very important process (the "Trace Coverage" feature). A process that many Hackers (especially those who are at the beginning of the road) omit it. They are simply not mindful (or aware) of covering their tracks and getting caught (in the US, by the FBI, CIA or the NSA) and punished in court for their deeds.

I repeat that **unauthorized access** to a system can lead to serious criminal consequences:

- confiscation of computer goods - laptops, external hard drives, etc.
- placing under supervision

G. REPORTING

Another very important step, especially in the Ethical Hacking process, is # 6, Reporting, the step in which Hacker generates a report on the vulnerabilities found (and exploited), the ways in which they can be corrected, and other information that will lead to solve and secure the system.

H. WEB HACKING USING THE BURP SUITE

The most powerful tool that currently exists online is “Suite.” Suite is an app that provides web services and penetration testing. When it is fully maximized, the possibility of its usage is almost limitless. Below are some of the features of the Burp Suite.

Intercepting Proxy is a feature that monitors and improves communication between an application and the web browser.

Spider is a feature that specifies all lists, names and characteristics of files that exist on a network.

Web Scanner is an important feature that scans for loopholes in the server.

Intruder is a feature that can be used to launch attacks against networks. It is used to scan for flaws and take advantage of them.

Repeater improves and makes solicitations on behalf of the user.

Sequencer examines the irregularity of the token’s CSRF, authenticity token, etc.

Extensions allow the user to include his or her own customized plugin or to install plugins directly from the systems database. They are used to creatively stage a tactical and cryptic attack.

I. WORDPRESS SECURITY & HACKING

By now, you should have some insight into what hacking is all about. Now we will outline the fundamental security guidelines that will protect you, your system and your information from external threats. All of the information we will provide is based on practical methodologies that have been used successfully. These methodologies will help prevent a computer system from being attacked and ravaged by malicious users.

Update Your OS (Operating System)

Operating systems are open to different types of attacks. On a daily basis, new viruses are released; this alone should make you cautious because your operating system might be vulnerable to a new set of threats. This is why the vendors of these operating systems release new updates on a regular basis, so that they can stay ahead of new threats. The best way to protect yourself from new threats is to update your operating system on a weekly or monthly basis. This will help you improve your security and reduce the risk of your system becoming a host to viruses.

Update Your Software

In the previous section, we talked about the importance of an update. Updated software is equipped with more efficiency and convenience, and even has better built-in security features. Thus, it is imperative that you frequently update your applications, browsers and other programs.

Antivirus

Based on our research, we have seen that some operating systems are open to a lot of attacks, especially Microsoft or Windows platforms. One way you can protect your system from viruses is through an antivirus program. An antivirus program can save you in many ways. There are many antivirus programs (free or paid) that you can install on your system to protect against threats. A malicious hacker can plant a virus on your system through the internet, but with a good antivirus scan, you can see the threat and eliminate it. As with any other software or program, your antivirus software needs frequent updates to be 100 percent effective.

Anti-Spyware

This program is also important, as you don’t want trojan programs on your system. You can get many anti-spyware programs on the internet; just

make sure you go for one that has received good ratings.

Go for Macintosh

The Windows operating system is very popular and therefore many hackers and crackers target it. You may have read articles and blogs saying that Macintosh operating systems are less secure; however, Macintosh is immune to many threats that affect Windows. Thus, we urge you to try the Macintosh platform.

Avoid Shady Sites

When you are browsing Facebook, you may come across unknown people who send you messages with links, some in the form of clickbait. Avoid clicking on such links. Also, you must avoid porn sites, or sites that promise you things that are too good to be true. Some of these sites promise you free music when you click on a link, while others offer free money or a movie. These sites are run by malicious hackers who are looking for ways to harm your computer with their malware links. Take note that on some malicious sites, you don't even have to click on anything to be hacked. A good browser will always inform you of a bad site before it takes you there. Always listen to your browser's warnings and head back to safety if necessary.

Firewall

If you are a computer specialist working in an organization, you might come across cases in which more than one computer system's OS is under one network. In situations like these, you must install software that provides a security firewall. The Windows operating system has an inbuilt firewall that you can activate and use directly. This firewall feature comes in different versions of Windows, including Windows XP, Windows Professional, Windows 10 and the other versions.

Spam

You can be hacked from spamming too. Email providers have taken the initiative to classify emails according to a set of parameters. Some emails will be sent directly into the inbox and some will be sent to the spam folder. To be safe, avoid opening emails that look suspicious. Some of them will have attachments that you should not open. Regardless of the

security measures taken by email providers, some spam emails will still pass their filters and come straight into your inbox. Avoid opening such emails and do not download the attachments that come with them.

Back-Up Options

Whether you are running your own business or working for an organization as an ethical hacker, it is crucial that you back up your work. Some files will contain confidential information, such as personal files, financial data and work-related documents you cannot afford to lose. You should register with Google Drive, Onedrive and other cloud drive companies so that you can upload your files as a form of backup. You can also purchase an external hard disk and transfer all of your important files to it. Take all these security measures because a single malicious software can scramble your data regardless of the antivirus you have installed. You can't reverse some actions once they've been taken, so always have a backup.

Password

This is the most important aspect of security. The importance of a strong password can never be overstated. Starting from your e-mail, your documents or even a secure server, a good password is the first and last line of defense against external threats. There are two categories of passwords: weak and strong. A weak password is made by using your mobile phone number, your name, a family member's name or something that can be guessed easily. Avoid using this kind of password, as even an amateur hacker can guess it.

Some people use dates such as their birthday or a special anniversary; however, that is still not safe. When creating a password, take your time and do some basic math because your password must contain both letters and numbers. You can even combine it with special characters. For instance, if your initial password is "jack," you can make it "J@ck007." A password like this will be almost impossible to guess even though it's simple. Furthermore, avoid writing down your passwords. Your password isn't a file that needs backup; it must be personal to you. Make sure you use a simple password that is very strong. However, keep in mind that a strong password still doesn't make you completely safe.

J. HOW TO DO GOOGLE HACKING

A few years ago, there was a standard way of transferring containers from virtual machines for software applications. One major reason for undertaking this process was to ensure flexible and cheap prices for the container in comparison to virtual machines. After many years of partnership with Borg and Omega container management, Google successfully implemented container know-how for running Google apps on massive platforms. By getting involved in libcontainer programs and enforcing cgroups, Google successfully enriched the container community. Google has achieved a lot by effectively maximizing container benefits for a very long time. After a while, Microsoft, which lacked VMs on its podium, corrected the deficiency by providing containers on its server.

Due to the fact that they are disclosed to a single point of failure, different containers cannot operate on a single host in a software test setting. The failure of a host will also affect the containers if they are operated altogether on that single host. To circumvent this, a container cluster is used. Google took that initiative and utilized a container cluster called "Kubernetes," which had an open source. Docker, on the other hand, invented a Docker swam solution, which is not yet fully accepted on the ground.

Another remarkable software or program is Microservices, which makes use of containers. A microservice is the simple usage of a web function that can be initiated more quickly than a standard web function. A way to achieve this is by grouping a unit of functionality in a single service and inculcating it into a simple web server.

Thinking deeply about the discussed factors, we can foretell that in some years' time, VMs will be routed out and completely replaced by containers. Some years back, experts worked together to carry out a container solution on the POC stage. However, some of the experts wanted to take the risk by testing them on manufacturing. As clusters develop over time, the current situation will change rapidly.

CHAPTER 3) CYBERSECURITY

A. WHAT IS CYBERSECURITY

Cybersecurity is the implementation of measures to protect systems, networks, and software applications from digital attacks. Such attacks are usually aimed at gaining access to confidential information, changing and destroying it, at extorting money from users, or at disrupting the regular operation of companies.

Implementing effective cybersecurity measures is currently a rather complicated task, since today, there are much more devices than people, and attackers are becoming more and more inventive.

B. BASIS OF CYBERSECURITY

What's the best way to secure a house against burglary? A typical burglar would scope out the premises beforehand to find the easiest point of access: a garage door that won't shut all the way or a second story open window, but a brash one might just walk to the front door and work the doorknob. The house owner who's been burglarized would then want to fix the garage door, put up iron bars on windows and install a brand new reinforced steel front door. All of this costs money, creates an inconvenience and, most importantly, attracts the attention of other potential burglars in the area – what is he or she protecting?

Securing the house thus becomes an endless game of cat and mouse, with time, money and effort invested on both sides to keep or gain **access** to restricted areas. The owner might ultimately conclude the best house security system is cheap, convenient and inconspicuous but there's no stopping a burglar who's well-funded, dedicated and left alone to tinker with a security system, so all security becomes just a deterrent. It turns out that securing a computer or a network follows the same principles as securing a house, but gaining access is easier than ever and the stakes are higher; we'll notice a missing microwave but a **hacker** , a remote cyberattacker with malicious intent, can steal all our data and keep stealing it for years without us even noticing.

C. MALWARE AND CYBER ATTACKS

Cyber threats come in many guises, from personal identity theft to corporate hijacking to institutional/national security hacks. As technology advances, it seems that the ranks of invaders—even computer terrorists—grow just as quickly. Basically, these threats break down into three categories.

Attacks on confidentiality: Credit card fraud is rampart in our world, as is identity theft. Both are criminal acts and inherent invasions of privacy; personal information is released to a potentially ever larger group of hackers, the person who was attacked must rectify the situation to great inconvenience. On a more public, more dangerous level are spies who focus on nations or states. Their activities focus on obtaining confidential data for military, economic or political gain.

Attacks on integrity: Integrity attacks, or sabotage, aim to damage or obliterate systems or information and those who use and rely on them. They can be as subtle as a typo or as blatant as an out-and-out smear campaign aimed to destroy the target.

Attacks on availability: The use of ransomware or denial-of-service are attacks on availability. The ransom comes into play when a price is demanded to decrypt the target's data, while denial-of-service swamps a network resource with requests, making the service unavailable.

More specifically, here are some ways that these attacks are carried out.

- A backdoor, also known as a cryptosystem or algorithm, is a way to bypass normal security controls such as passwords. They can be authorized (as for a specific purpose) or added by an attacker. In any case, they create a vulnerability.

- With the goal of making a computer or resource unavailable, denial-of-service attacks can occur when incorrect passwords are entered multiple times, thus locking the account, or by overloading the system with

requests and blocking all users. These attacks can stem from zombie computers or even from duping innocent systems into sending unwanted traffic.

- Eavesdropping is exactly what it sounds like—listening to private communications between network hosts. Certain programs are used by government agencies to "audit" ISPs. This widespread practice extends to closed systems when electro-magnetic transmissions are monitored.

- Masquerading through falsifying data in order to gain access to unauthorized data is called spoofing and comes in many forms: email spoofing, forgery of a sending address; MAC spoofing, changing the Media Access Control address to pose as a valid user; biometric spoofing, faking a biometric sample; IP address spoofing, altering the source IP address to hide identity or impersonate another system.

- Through physical access or direct-access attacks, a perpetrator can copy data, compromise security, install listening devices or worms and more. Even protected systems are vulnerable to this type of attack.

- Phishing frequently uses email spoofing or instant messaging to direct a user to enter confidential information by looking almost the same as the legitimate site.

- Through privilege escalation, an attacker can escalate their access level by fooling the system into granting access to restricted data or resources.

- Clickjacking is literally hijacking a user to click on a link or icon to another website other than the intended one. Particularly sneaky, clickjacking routes the clicks,

or sometimes keystrokes, to an irrelevant page.

- By impersonating an institution, bank, customer or other entity, social engineering leads users to reveal passwords, credit card numbers and other private information. This scam reportedly costs U.S. businesses more than $2 billion every two years.

Without computers, the world would slip back into pre-Industrial Revolution mode. Technology has streamlined every aspect of life, particularly for businesses and other public entities, some of which are more and more at risk.

Financial systems: Financial regulators, investment banks and commercial banks attract cybercriminals who see an avenue to market manipulation and illegal gains. Any website than enables transfer of funds or buying goods is also a target, as are ATMs, which are frequently hacked for customer data and PINs.

Utilities and Industry: Vital services including the power grid, nuclear power plants, water and gas networks and telecommunications are controlled by computers. It has been proven that even those controlled by computers not connected to the Internet are vulnerable to attack.

Aviation: One power outage at a major airport can have a tumultuous ripple effect on air traffic. Radio transmissions would be disrupted, an in-plane attack can occur, loss of system integrity and aircraft, and air traffic control outages are just some of the possible outcomes.

Personal devices : All of those wonderful gadgets that people use to simplify life—smart phones, tablets, smart watches, activity trackers—can be exploited through built-in cameras and other devices. Attackers can collect health other personal information or use the device networks as

paths to an attack.

Corporations: Identity theft and data breaches such as credit card information have been aimed at large corporations such as Target Corporation and Equifax. In some cases, foreign governments attempt to spread propaganda or spy through attacks. Health insurance fraud, which costs everyone, and impersonation of patients to obtain drugs for illicit purposes, are also common. Despite these activities, 62% of all organizations did not augment security training in 2015.

Autos: Today's vehicles practically drive themselves, and the day when this common is not far off. Cruise control, airbags, anti-lock brakes and other features make driving more enjoyable and, hopefully, safer. WIFI and Bluetooth keep the cars connected and raise the possibility of security breaches.

Government: Attacks on government and military systems create chaos, disrupt services and—to the extreme—qualify as acts of terrorism. Whether it is an activist, foreign government or other hackers, the result is infrastructure malfunction of personnel records, police and other first responder communications, student records, traffic controls and financial systems. Widespread computerization of personal identity items such as passports and access cards also lead to vulnerability in this area.

Internet of things (IoT): Physical objects that carry sensors, software or any type of network connection to store and share data are part of the Internet of things. A building, vehicle or appliance can comprise the IoT, and the proliferation of this modern phenomenon creates the possibility for physical—not just virtual—threat. For instance, a stolen cellphone can unlock a residence or hotel room door.

Medical systems : Viruses, breaches of sensitive medical data, diagnostic equipment, and other devices are potential targets of attacks. These threats are deemed so likely that, in 2016, the U.S. Food and Drug Administration

created guidelines for secure maintenance of manufacturers of medical devices. However, no recommendations or structure for implementation were included.

Malware

Malware of one type or another, is the single largest threat to the average organization's daily operations, offering the potential to directly impact the availability of critical data and assets. As such, if they hope to combat this threat effectively, organizations both big and small need to increase their vigilance while at the same time evaluating their capabilities when it comes to response, detection, preparation and planning for potential threats. As new types of destructive malware are certain to evolve over time, it is critical to not just understand how your organization is going to prepare for known threats, but how it will prepare for the unknown as well.

Distribution vectors: Potentially destructive malware frequently has the ability to target large-scale systems that can then potentially execute simultaneously at multiple points throughout a given network. As such, it is crucial that organizations regularly asses their operating environments for atypical channels that could indicate potential malware propagation or delivery. Systems worth keeping an eye on include the following.

- Enterprise applications, especially those that have the potential to interface directly with multiple hosts and endpoints. Common examples include patch management systems, asset management systems, remote assistance software, antivirus software, centralized backup servers, file shares, and network administrative systems.

- While not limited to just malware, the following threat actors could compromise resources that would ultimately impact the availability of critical applications. Potential threats of this type including centralized storage devices,

high risk partitions or data stores, network devices, routing tables and crucial network resources.

Strategies for success: While there are plenty of potential malware vectors that the average organization needs to deal with on a regular basis, there are also numerous different strategies that make keeping malware at bay far more manageable. The first of these is ensuring a viable communication flow at all times.

It is also important to ensure that your flow paths for communications are not only well defined but authorized or documented as well. From there, you will want to strive to increase awareness of systems that can be utilized as a gateway to laterally pivot as needed or directly connect to relevant endpoints found anywhere throughout the enterprise. Whatever you do, it is important to do what you can to ensure that these systems are maintained within these restrictive VLANs with appropriate network access control and segmentation as needed.

When it comes to ensuring the right amount of control over who has access to what, it is important that enterprise systems that can interface with numerous endpoints directly all require dual-factor authentication for any interactive logins. Further, it is important to make sure that authorized users are limited to a specific subset of the organization's personnel. Whatever you do, it is important that the default user group doesn't have the ability to authenticate or access these systems directly.

You will also need to ensure that unique domain accounts are documented and utilized for every service that involves and enterprise application. The context in which these permissions are assigned to various accounts should always be fully documented and also configured in such a way that the greatest number of users have the fewest number of privileges possible. Doing so provides the enterprise the ability to track and monitor actions that are taken based on assigned service accounts.

This is why it is important to avoid providing a service account with either interactive or local login permissions. In fact, service accounts should be expressly denied these types of permissions, especially if access to critical data locations or important network shares. Additionally, accounts that are used for the purpose of authenticating centralized servers should not contain downstream systems that have elevated permissions as this could allow a system that is far easier to compromise to infect a system that is typically far better protected.

Recovery planning: A business impact analysis is a crucial component when it comes to preparing a contingency plan in case your system is attacked in a serious way. This plan should provide your organization with two key components, interdependencies and a classification and characterization of relevant components. To plan for this type of scenario, an organization is going to need to address the accessibility of available resources including mission critical applications and systems, contact information for crucial external contacts, contact information for essential personnel and a secure communication channel for each. It is also important to have all major vendor contact details, points of contact when it comes to organizational procurement and back up ISO files for all critical applications and systems.

Containment: If an organization experiences a large-scale outbreak of malware, the immediate focus should be on containment above all else in hopes of reducing the scope of the attack overall and minimizing the likelihood that additional systems are going to be impacted. To develop a strategy for containment, the best place to start is by determining the vector or vectors that are common to all of the systems that are experiencing problems that could have been used to deliver a malicious virus. Common options include

- DNS Server
- Network boundaries or segments

- User accounts with higher than average privileges
- Centralized file shares
- Centralized applications

Once you find a likely distribution vector, you can then move on to enforcing additional means of mitigation, starting with implementing network control lists as a means of denying applications the capability of communicating directly with other systems. Doing so will immediately make it much easier to isolate and sandbox specific resources so that you can more accurately determine what's wrong. Your internal DNS can be used for this task by simply adding a null pointer to the DNS zone for any identified applications or servers which will make it easy to see what both are running and unidentified.

D. FIREWALL AND WHAT ARE YOUR FIREWALL OPTIONS

It is an internet filtering measure, was bypassed using encrypted PDF files sent as email attachments that could both contain commands and harvested data, such as email content and metadata. These PDF files could be opened with a PDF viewer but contained only a 1x1 pixel white image, displaying a single blank page. Automated email management systems legitimately present in Outlook were used to hide these command&control emails, so a user watching at his inbox intently could spot only a flicker of an email before the exploit deleted it without any record. Desktop notifications were also blocked. The exploit came with a list of preset email addresses where it could report back to Turla but also had a way to add backup email addresses in case the original ones were taken down.

By all accounts, Turla was a state-sponsored hacker group since their goal was mainly surveillance and monitoring rather than immediate financial gain. They showed a great deal of patience and skill, using custom encryption methods to buy as much time as possible when their exploit was ultimately discovered. An entire suite of Turla malware was eventually discovered. Among them were Trojans, used to deploy the

Outlook exploit, such as Gazer[31] , where the authors even put in some video game references in the code. Malware was used against states before, and this exploit was fairly tame compared to **Stuxnet** , the world's most famous cyber-weapon.

E. WHAT YOU NEED TO KNOW ABOUT CRYPTOGRAPHY AND DIGITAL SIGNATURES

The problem with cryptography and hashing, in general, is that once deployed, these algorithms stay still, but the computing power advances and makes it more likely the security of these measures will be breached. So, using older software becomes a gamble that's more and more likely to wipe you out as time goes on, but updating isn't always the best option since it costs money and disrupts your workflow. You don't have to feel obliged to update to the very last version of software as soon as it comes out – unless others are depending on you.

On the other hand, companies certainly should do as much as they can to tighten their cybersecurity efforts and stop data leaks, which are a frighteningly common occurrence. When your computer gets hacked, you can lose banking data but just as easily call the bank to reverse any given transaction; when Facebook gets hacked, millions of people will have their most intimate data, from chat conversations to photo albums exposed to hackers and possibly exploited at some point down the line.

Hospitals and airports are very vulnerable targets that we don't think about until they're hit with **ransomware** , malware that locks up the system until some money is paid to the hacker, usually cryptocurrency. In May 2017, WannaCry ransomware hit over 200 thousand computers across the world, including those in hospitals, banks, and airports. Some of these institutions used Windows XP way past its support date, making it trivial for hackers to waltz into an office, plug in an infected USB and lock down their entire network. Who made WannaCry? It was supposedly a hacking tool made by the NSA, stolen by a hacker group and repurposed for theft.

In any case, hardware and software failures **will** happen; hence, the smartest move is to back up your data, which is the only surefire way to protect against hacking. Separate the original and the backup as much as

possible, preferably by having one on the cloud and the other on an external hard drive that's disconnected from the internet. Include photographs, voice messages and other personal trivia in your backup, so these precious memories don't get lost due to a hack.

F. WHAT IS A VPN AND HOW TO USE IT FOR YOUR OWN SECURITY

Most users nowadays have routers, which connect the devices like mobiles, tablets and computers to the Internet. The router will be given a public IP address by your Internet service provider and each of the devices that connect to the Internet will be given a private IP address. The router gives the private IP address. Whenever you connect your computer to the Internet, it will look like your computer is your router. In cases where the users have only a single computer, they can connect it directly to the Internet and their ISP will give a public IP address to it. Since the assigned IP address is public, a host from the other end can track your Internet activities.

VPN (virtual private network) allows the users to connect to another network. The VPN will provide your computer with its own IP address. VPN can be used for hiding your original IP address and your IP address provided by your ISP will be hidden. VPNs are not just used for hiding IP addresses. You can access any network from your organization, which may be blocked from certain networks. There are many commercial and free VPN and proxy services available on the Internet. Using these you can connect to the Internet with a new IP address and your original IP address will be hidden.

G. TOR BUNDLE AND PROXY CHAINS

Linux supports the classic multiprogramming scheme. Linux supports parallel (or quasi-parallel if there is only one processor) user processes. Each process runs in its own virtual address space, i.e. processes are protected from each other and the collapse of one process will not affect the other running processes and the system as a whole. One process cannot read anything from the memory (or write to it) of another process without the "permission" of another process. Authorized interactions between processes are allowed by the system.

The kernel provides system calls for creating new processes and for managing generated processes. Any program can start executing only if another process starts it or some interruption occurs (for example, an external device interrupt).

In connection with the development of SMP (Symmetric Multiprocessor Architectures), a mechanism of threads or control threads was introduced into the Linux kernel. A thread is a process that runs in virtual memory, used together with other threads of a process that has separate virtual memory.

If the shell encounters a command corresponding to the executable file, the interpreter executes it, starting from the entry point. For C programs, the entry point is a function of main. A running program can also create a process, i.e. run some program and its execution will also begin with the function main.

H. ADVANTAGES OF CYBERSECURITY

When it comes to the importance of ensuring the cybersecurity of your portable devices, only you can accurately determine what's at risk besides the machine itself. However, with most portable devices these days, if the thief is able to access the information that is stored within it successfully, a lot more than the data directly on the device itself is at risk.

You have likely heard stories about the uproar caused when a senior manager for one major corporation or another leaves a laptop or a smartphone somewhere they shouldn't. Confidential information of this type can cause untold damage to a company, especially if it has something to hide. Even if your devices don't have serious secrets hidden within, there is still enough on the average smart device to make your life very difficult if the wrong person gained access to it. Keep the following in mind when it comes to keeping your data private on the go.

Password protect everything: It doesn't matter if it takes you an extra 30 seconds to access your device, this one simple step is responsible for decreasing the likelihood that your device is accessed by the wrong person by more than 100 percent. It's easy, readily available and an option when

you set the device up for the first time, there is no reason not to take full advantage of it.

Treat your property as valuable: With smart devices so ubiquitous, it can be easy to be flippant about them when you are out and about, especially if you are busy or otherwise in a hurry. Regardless of the personal cost of the device in question, it is important to not just think about the physical value if the device was lost but the value of the time wasted in changing literally every password and credit/debit card you own. Furthermore, think about the potential value of keeping your identity secure and act accordingly.

Likewise, you should make a habit of keeping an eye on your surroundings when using your device, which will likely be easier said than done. Nevertheless, you should try and pay attention to those around you, including anyone who may be trying to look over your shoulder for a peek at your sweet, sweet data. Generally speaking, if you don't need your device at the moment, it is best to keep it hidden away from prying eyes, just to be safe. If you are using a company laptop, you may even want to consider a third-party alarm that can be set to ensure that anyone who tries to access the computer without your permission is in for a rude awakening.

Regardless of how important your information is, it is important to have at least one backup of all your data stored in a secure location or, more likely, the cloud. This way you will be able to ensure you are able to get back to where you were as quickly as possible, you will also know exactly what information is now at risk, allowing you to take additional precautions as needed.

What to do if your device is stolen: The first thing you are going to want to do is report the theft to the proper authorities as they may have procedures in place that you might not be aware of for this sort of thing. It is also important to cancel any mobile data service that is on the device as quickly as possible to delay the culprit as much as possible and give yourself time to change all of the relevant passwords in the interim.

Ensure your data is secure

Add additional layers of protection: While there are naturally going to be innate security options for portable devices, their very nature means they are more likely to be targeted than anything else you own which means it is important to take as many security precautions as are warranted for the type of data you are typically transporting. It is also important to keep in mind that if your device is going to be connecting to an unsecured network connection then it is vulnerable to network attacks as well and plan accordingly.

Store important data separately: There are a wide variety of extremely secure external storage options available these days which means there are plenty of ways to keep your sensitive data safe from prying eyes, and completely separate from the devices that are most likely to be targeted for theft. Despite the prevalence of storage space, this option is used far less frequently than it should be which means you will have the advantage of being unexpected on your side as well. You can even keep the data in a pocket on your person at all times, virtually ensuring that you know where it is at all times.

Don't rely on passwords alone: If you are dealing with sensitive files, don't trust passwords alone to defend it. Instead, take the extra step of encrypting them and ensuring that even if your device ends up in the wrong hands the data is still largely secure. By adding an extra layer of encryption, you ensure that unauthorized people won't view the data, even if it physically falls into their hands. Keep in mind that it is very important to keep a list of these passwords, and to ensure that said list is not directly accessible from your computer to avoid making the whole thing pointless.

Ensure your virus protection software is up to date: Unlike personal computers which are far more likely to remain on, and thus receive automatic updates, portable devices, especially those provided by the company, tend to be used on a more sporadic basis which means ensuring everything is updated regularly is going to be your responsibility. Make a

habit of checking for new security updates once a month, and also ensure that the virus and spyware software available on the device is up to date as well.

Maintain a strong firewall: While a firewall is a good idea when it comes to securing your personal computer, it is even more important as your portable device is going to be connecting to a wide variety of different networks, very few of which you will be able to tell are secure with any degree of certainty. If you are going to be using your device while traveling you are going to want to ensure your firewall settings are set to the highest settings at all times, just to be safe.

I. NETWORK MANAGEMENT AND A LOT OF METHODS TO SPOOF ADDRESSES

There are several things that you can do to get into a network using your hacking abilities.

Ping

Every Wi-Fi has an IP address that is assigned to it. Even the computer that you use to hack into someone else's system is going to have an IP address.

An IP address is going to be a series of numbers that is unique to that router. However, the IP address alone is not going to tell you much on its own.

To convert the address, you are going to use the ping option. The DNS is also going to help to get the name of the domain. Ping is going to stand for packet internet groper and is going to be on all versions of Windows that their clients are going to use.

After you have logged into the internet, you are going to need to need to open up the shell for DOS and then insert a command for ping. This is going to look for the domain name and then display it on the computer that you are using.

The use of ping is going to usually be the first step that you are going to take when you are trying to hack into a network. The ping is going to reach out to your target and tell you if it is online or offline.

Multiple IP addresses are not going to be able to be converted into domain names. When you are wanting more control of your ping, you are going to use ping commands.

Ping sweep

This is going to involve ping, but instead of using it to get into a system, it is going to search the IP addresses that are open in a specific area around you. Using this is only going to be useful when you are not sure where you want to attack therefore you are going to know where you can get into without necessarily knowing who the target is or even where they are located.

Tracert

This program is another tool that is going to get information about the host no matter how remote. It is going to use ICMP.

Tracert is going to locate data by sending out packets from the source computer to the computer that is the target. The computer that is being used for hacking is going to get an IP address sent back to it after connecting and is thus going to reveal all of the stations that are going to start with the connection that you have to the internet.

Should the name not be able to be revealed with ping, then this program is going to be able to give it, or even the last station that the attacker visited. This can end up causing concern when it comes to the name of the internet provider that the hacker is using and where they are located.

Port scanning

At the point in time that the system that has been targeted is listed online, the next thing to do is to scan the system for any open ports that can be used to get in.

The port scanners that you can choose from is going to be numerous and they can be found online. However, most of these scanners are going to

use techniques that are going to end up getting the hacker caught because they are outdated.

Nmap is not going to only scan all the ports that are open on a system, it is also going to tell you the operating system and the version numbers of the programs that are being used on that computer.

Common ports

There are some of the more common ports that are going to be opened for hackers to get into and in this list, you are going to find not just the port name, but the service that normally runs it.

- 445 SMB it is going to use NetBios instead of TCP unless it has to use TCP
- 20 FTP Data it is used mostly for file transfers.
- 443 SSL a secure layer for the sockets
- 21 FTP another one for file transfers
- 389 LDAP
- 22 SSH
- 220 IMAP3 this will use the internet message access version 3
- 23 Telnet
- 194 IRC which is used for the chat that is going to go between the computer and the internet
- 25 SMTP mail transfers
- 161 SNMP a network management
- 53 DNS the domain name
- 143 IMPA the internet message but it is not going to be a specific version
- 68 DHCP the host for configuration
- 139 NetBIOS

- 79 Finger
- 137 NetBIOS-ns
- 80 HTTP
- 110 POP3 the post office protocol version 3 is going to be used.

CHAPTER 4) KALI LINUX

A. WHAT IS KALI LINUX

To get started with wireless hacking, one must first become familiar with the tools of the trade. No single tool is more valuable, especially to a beginning hacker, than Kali Linux. A free, stable, well-maintained, and astonishingly complete set of analysis and penetration software, Kali evolved in the crucible of open-source Linux distributions and has emerged as the king of all hacker operating systems. This successor to the notorious BackTrack distribution has everything that a hacker needs, from newbies to hardened experts.

B. HOW TO INSTALL KALI LINUX

The most convenient way to use Kali Linux long-term is by installing it on your hard drive. You can install Kali Linux alongside other operating systems such as Windows, MacOS, and other Linux distributions.

To install Kali Linux on the hard drive, we are going to require several tools.

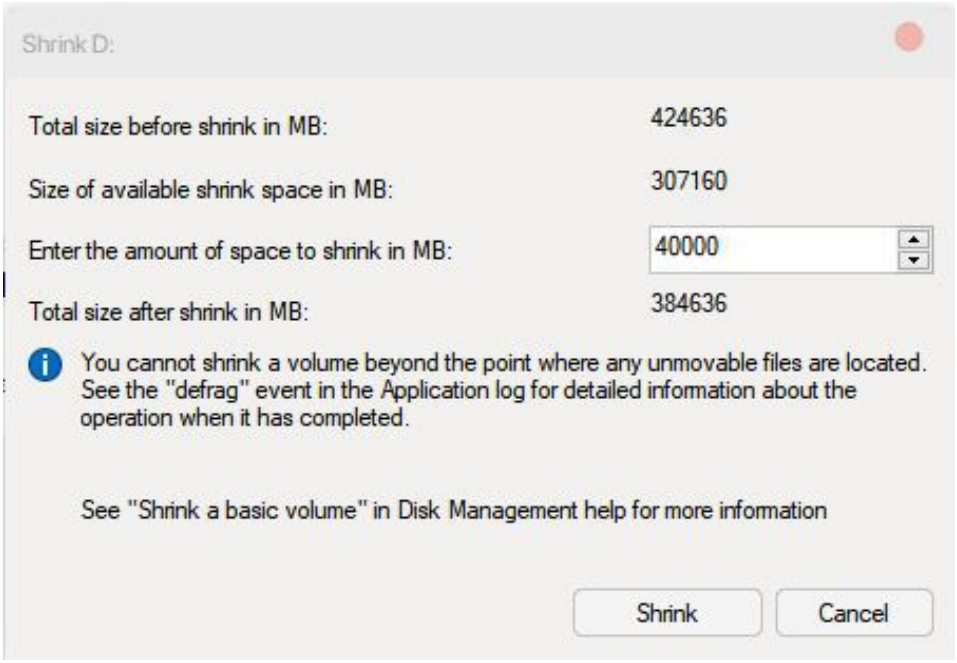
They include:

- ❖ USB/DVD bootable media
- ❖ A minimum 20GB disk space for Kali Linux installation
- ❖ Kali Linux ISO – obtained above

Installation of Kali Linux on a physical machine requires a clean, non-partitioned hard drive without any data in it. Here, we are installing Kali alongside another operating system.

Once you have obtained a media device such as USB or DVD, it is time to create a bootable disk. If you are using a USB flash drive, download and install BalenaEtcher tool and follow instructions to burn the image.

Once you have created your bootable media, you need to create a partition for Linux partition. If you are using windows, open disk manager, select the disk to partition, and click shrink volume. Set the size of the partition —it must be 10 GB and above—and click shrink.



Once you have allocated your partition size, boot your device using the created bootable media above.

NOTE: Different computer models have different boot configuration. You can search the internet for your device boot options.

Once your system boots, Kali Linux will prompt you with the following boot menu window.

Choose the method of installation. The graphical installer is the friendlier to beginners. Select and configure your preferred language of installation. Next, select your geographical location. The next step is to configure your keyboard settings. Follow this with setting up your network settings and connect to a network. After that, create a password for the root user, which is a MUST-do. Continue to setup user account and password.

On the next screen, which is the partition part, select ‘use the largest continuous disk space’ and select the partition you created earlier. Confirm and allocate the disk space, and then select ‘write changes to disk.’ Select ‘yes’ and click continue. Wait until the installation process completes.

The next step is the package manager. Select ‘yes’ and click continue. If you select yes, make sure your device has an active network connection. If not, select no.

Next, install the GRUB bootloader on to the disk. Once the installation has completed, reboot the computer and select Kali Linux in the GRUB menu.

C. INSTALLATION OF VIRTUAL MACHINE VM WARE

Advances in processor speed, the advent of multicore and multiprocessor chips, increased memory size, and increased data storage have made hardware virtualization a viable and practical means of running multiple software platforms on a single computing device. Running operation systems within a VM has advantages because it eliminates the need for multiple pieces of expensive hardware and makes the use of highly specialized distributions such as Kali practical. In addition, using penetration testing software within a single host allows hackers to practice attacks in a safe "sandbox" environment, targeting various other VM's within the host. The downside of using an OS within a VM is that there is competition for host resources, and the virtual hardware capabilities are limited to those of the host machine.

Functional and feature-rich virtual machine software is available free of charge. The most common free VM applications are **Virtualbox** and **VMware Player** (which has commercial versions with additional features). **QEMU** is an open-source option that runs solely on Linux. This book will use Virtualbox to demonstrate a virtual Kali installation because it is available for Windows, Macintosh, Linux, and even Sun systems.

D. HOW TO WORK WITH KALI LINUX

This kind of operating system is known as a distribution and it is designed for penetration testing and security auditing. It is meant for a single user at a time. This limits the potential for security breaches.

In fact, this system is very particular about security, since it is designed for people who work in information and network security. It can be modified to allow for more users and to become compatible with many programs, but that isn't advisable. That can compromise the security of the system, which defeats its purpose.

It is recommended that you work within the parameters of the Kali Linux system so as not to allow in any potential security breaches. Because it is such a closed system, it won't be compatible with programs that permit a lot of online interactions or open sourcing. So Steam won't work with it at all, nor will Launchpad and many other commonly used programs. If you want to run those programs, then you should really use a different

operating system that isn't designed to be as narrowly focused as this one is.

If you try to install additional programs on Linux that connect to a network, such as Bluetooth, then you won't have much luck. These kinds of services are disabled under the default settings used by Kali Linux. The distribution is intended to remain secure, and unless you tamper with the settings it will stay that way, even to the detriment of the programs you want to use on it.

You can tamper with the program as much as you like, opening it up for compatibility with just about anything, since it runs off of Linux. But that's not a good idea if you want to maintain security. As you get more used to how it works, you can do more with it and modify it as you like, but when you first start out, you probably shouldn't try to tamper with it. Wait until you are more familiar with it to start doing high-level modifications.

E. HOW TO START HACKING WITH KALI LINUX

Depending on the needs of the user, they may wish to build their own Kali Linux ISO using the available tools. Building your own ISO can be rewarding as this allows the user to fully customize their build, rather than relying on the pre – built downloads. Most of these modification builds are done using Debian live – build scripts, given that Kali Linux is built on the Debian Linux core. These scripts allow the user to automate the process of building a live system image by creating a framework for the configuration set to be able to build the needed image.

The custom ISO of Kali Linux should preferably be built within a pre – existing Kali Linux environment, in order to ensure that all assets, packages, and libraries used are drawn from the verified Kali Linux resources, ensuring that the build remains safe and secure, given the stringent security protocols used in order to build Kali Linux.

F. EXPLAIN ALL THE BASIC CONCEPTS TO KNOW BEFORE START HACKING

Given the short background of Kali Linux as discussed earlier, it would be beneficial for the reader to have a short overview of the features and

specific capabilities of Kali Linux, which should give a clearer idea of what Kali Linux really is and how it is used.

Expansive library of network security and penetration testing tools: Kali Linux found its origins from Backtrack, as previously discussed, and thanks to this, there have been a huge amount of tools developed over time for the Backtrack distribution. However, due to the passage of time, a lot of these tools have been rendered redundant or outdated, and the Kali developers have been able to cut these down, removing the tools that no longer serve the intended purpose, while integrating and adding new and updated tools.

G. INSTALLATION OF VIRTUAL MACHINE VM WARE AND INSTALLTION OF KALI LINUX IN DETAIL

For Kali Linux to be run "live" on standard Windows – OS or MacOS based – computers running on Intel processor chips, the user has to make sure that they have a Kali Linux official bootable image, which is available in both the 32 – bit and 64 – bit format.

In case the user is not entirely sure of what architecture they will be running Kali Linux on, if they are operating on Linux or OS X, for example, the command " uname – m" on the command line should return either "x86 _ 64" or "i386". In case of the "x86 _ 64" result, this means that the 64 – bit format should be used, which is the one with "amd64" in the ISO file's name. Otherwise, the "i386" result means that the 32 – bit format should be used, with "i386" as the identifier in the ISO's name.

For Windows users, the system architecture is easily verifiable by checking the system configuration through the control panel.

Kali Linux ISO files are downloadable directly though the official Kali Linux website as ".iso" or ".img" formatted files, or through a ".torrent" file, though the latter would require the use of a torrent application.

Kali Linux ARM Images

ARM – based devices vary widely when it comes to their hardware architecture, thus it is impossible, or at the very least massively impractical for Kali Linux to have an image that can plug – and – play across all ARM – based devices. However, there are pre – built images of

Kali Linux for a lot of the more popular ARM – architecture based devices, and the user may check to see whether or not their device is on that list. Failing that, there are scripts available for the user to build their own ARM images, which can be found on sites such as Github. The user may also wish to refer to other guides when it comes to establishing an ARM cross – compilation environment or setting up a custom Kali Linux Distribution ARM ch root.

H. BASH SCRIPTING

Providing your website with adequate protection from a hacker is more important than ever before. The website owner must give visitors a safe surfing environment. Adequately securing the website protects it from being infected with malware, protects your visitor's details, improves your web ranking and ensures you continue doing business for a long time. Keep in mind that once your website is hacked, it is very difficult to put it back together. You will lose customers when your website goes down and your reputation will also be lost.

We have talked about the various flaws that can be exploited on the server and client sides of a website. Some of these attacks are very difficult to detect and that is why prevention is the best policy.

If you run a website based on a content management system like WordPress or Joomla, always install security plugins that are available on that CMS. Sitelock is a valuable tool that scans a website daily for flaws, malware and viruses. Investing in a good cloud protection service is also a great idea, as it will filter all of the content that reaches the site and screen out suspicious traffic and bots.

One of the most popular and commonly executed website attacks is the SQL injection. Exploiting this flaw gives a hacker access to private information. This type of attack is executed on websites that have form fields which accept user input. A very good way to prevent this attack is to use parameterized queries. This ensures the website contains parameters that make it impossible to insert malicious codes.

We also talked about cross-site scripting attacks, or XSS attacks for short. We now know that cross-script attacks are a result of JavaScript codes that are executed in the client's browser. As with the SQL injection attack,

preventing the XSS attack requires that the programmer or developer state explicitly what entries are allowed in a browser's various user input fields. A great way to do this is by implementing a content security policy, or CSP for short. This will give directions to the browser for different entry fields, including which field should allow for executable scripts and which should not.

For websites that require user login information, it is important to insist on strong passwords when the user registers. Users should create a password that is a mixture of letters, numbers and special characters or symbols. It is also important to ensure that passwords are encrypted when users log into the website. This measure makes it difficult for hackers to crack the password if they happen to execute a man-in-the-middle attack. Also keep in mind that it takes just one weak password for a hacker to gain access to all of the accounts.

Also ensure that user inputs are properly validated when they are typed in and when they are sent over to the server. This client side and server-side validation ensures that malicious codes are not mistakenly executed. Regarding the browser, on the web page, it is important to define the fields that require input and to also make sure they follow the input field specification. A field that is meant for numbers should reject a letter or a special character input before the content is sent to the server for another phase of input validation.

If you run an e-commerce store, a banking app or any other website that accepts and stores very sensitive information, get an SSL certificate. This provides an extra layer of security for your website. Customers and clients who visit your site will rest easy when they see that "HTTPS" precedes your website URL. This HTTPS encrypts all the information traveling to and from your server. It renders any information being sought by a hacker as useless even if he or she is performing the sniffing attack.

Error messages displayed to the user should be kept minimal. If an error message is to be shown to the user at all, it should not include vital information like the database type or error code. It is a good idea to configure the error message to display a generic message because error messages give a hacker information about the underlying structure of the website or web app, which can be used to coordinate a targeted attack.

It is also important that your admin username and password are very strong. Make sure there is a limited number of login trials on the login page. Ensure that security questions are asked when a user uses the “forgot password” link. Even if the user gets the question right, avoid sending the login username, password or other credentials to the user's email.

Make sure you set strict permissions that need to be granted before anyone can access your files. Ensure that only the admin can edit some files, while keeping other files readable for the website’s users. It is also a useful practice to limit the number of files that can be uploaded on your website. Through file uploads, it is easy to embed malicious codes that can open up a website to attacks. Make sure that all uploaded files are saved in a private folder and can only be shown by executing a script written solely for that purpose. Furthermore, you should not allow the uploaded files to reach the root folder.

As with web apps and websites, it is important that we ensure that when coding or working with programmers on a project, we adopt what is known as secure coding practice. Examples of secure coding practice include designing a system for maximum protection against hacks, building each module separately, testing modules for flaws and merging everything together so that the entire application can be tested for other vulnerabilities.

It is also a good policy to keep designs as simple as possible. Complex websites or web app designs are more prone to errors and issues that a malicious user can take advantage of. As mentioned throughout this book, data sanitization is very important for securing your website or web app. Always sanitize the data that is flowing through your application, whether it is coming from the user, the server or even a third-party-linked application.

CHAPTER 5) HOW TO HACK WITH KALI LINUX

A. HOW TO START HACKING WITH KALI LINUX

While Kali Linux is used by security professionals all over the world and is a highly specialized version of Linux, it won't cost you anything. The developers vow that it will always be free, even as they continue to provide support and updates for their version of Linux. They also make sure that modifications are not being made to the OS by just anyone.

What Kali Linux Does

This kind of operating system is known as a distribution and it is designed for penetration testing and security auditing. It is meant for a single user at a time. This limits the potential for security breaches.

It is recommended that you work within the parameters of the Kali Linux system so as not to allow in any potential security breaches. Because it is such a closed system, it won't be compatible with programs that permit a lot of online interactions or open sourcing. So Steam won't work with it at all, nor will Launchpad and many other commonly used programs. If you want to run those programs, then you should really use a different operating system that isn't designed to be as narrowly focused as this one is.

B. STEP BY STEP SPPROACH ON HACKING WITH KALI LIUNX

By now, we should have a good idea of what Kali Linux is used for, and what "white hats" are, and ethical hacking. In addition, we have already gone over how to make sure that the Kali Linux that the user is downloading is verified and safe, with no malware or any other modification that would compromise its security. We now also know how to build our own installer image and package of Kali Linux, customizing it to our needs. We've already gone over how to install Kali Linux, and even dual – boot it, in case we need such a feature. Now we can go on to some of the basics, how to actually use this program that we've learned about, downloaded, and installed.

C. STEP BY STEP GAINING REMOTE ACCESS

Wifi hacking is one of the most basic forms of hacking, and is usually taught to beginner white hats to get them familiar with the process. The first step is to find a wireless network to hack: remember that "just trying" or "I'm learning" is not an excuse, and any unauthorized access or attempt to access without authorization may be punishable, so best that you ask permission, or better yet, simply create your own wireless network for convenience.

Now that we have a wireless network to work with, the next step is to find out the name of your own device's wireless adapter. Note that there are a couple of terms that we should be familiar with: "eth – ethernet", and "wlan – wireless local area network". The "wlan" is what we're looking for, so keep an eye out for that. Boot up your Kali Linux terminal and type in ifconfig, which should show us a lsit of all the terminals of our computer. Take note of the "wlan" adapter, along with the suffix, which is usually 0 / 1 / 2.

Now that we have our wireless adapter, we now have to enable monitor mode. The user can employ a tool called airmon – ng to create a "mon" virtual interface. This can easily be done by typing

Airmon – ng start wlan0

This should create a monitoring interface, which would be named by default as - mon0 if using an earlier version of Kali Linux, but if using the Kali Linux 2.x onwards, the name would be wlan0mon.

Once the monitoring interface is up, we can begin to attempt to capture data packets that are being transmitted by the wireless network that we are trying to crack into. The following tool should help us gather data:

Airodump – ng wlan0mon

That should allow us to access a few data packets. If we want to save the data in a file, which we do, we add another command to the end, "write *filename*", so it should look like the following:

Airodump – ng wlan0mon - - write *filename*

That will store any captured packets in *filename*.cap. Once we have about ten thousand data packets minimum stored, we can proceed with the wifi cracking process.

Now that we have our data packets, we can open another terminal and type in:

Aircrack – ng *filename*-01.cap

This should begin the cracking process, or, if there are multiple wireless networks, the program will ask which wireless network will be the target of the crack. Note that if there are multiple wireless networks, the amount of captured data packets needed may be even higher. If the password is fairly weak, then the password should appear in the following format:

Xx :: xx :: xx :: xx :: xx :: xx :: xx …

Remove the colons (so it will be "xxxxxxxxx"), and that should be the password of the wireless network. If the data packets captured aren't enough, then the program will tell you so, and you have to gather more data packets to have enough to crack into the wifi.

One of the more common attacks, as earlier discussed, is SQL injection in order to gain access to a website or a database. Though the reader should know this by now, just for review: SQL is a structured query language that allows the computer to manage data, in order to store, manipulate, and retrieve data from the server or system database. The database is the repository of all the data, often containing passwords and other sensitive information.

So what is SQL injection? SQL injection is a way of injecting queries into the database. Now the database is specifically meant to answer queries, but only from authorized sources. SQL injection is a method wherein external queries, from unauthorized sources are granted access to the database. This is done through "inserting" them into the normal flow of data queries in order to disguise them as authorized requests for information. This allows the hacker to retrieve the information in the database, whether it be passwords, encryption keys, or even raw data. There are also some SQL injection methods that not only allow for retrieval of information, but even insertion of malware or other files, which may allow the hacker in

question to control the database, either locking out the owner or even deleting some or all the files within. Needless to say, SQL injection is one of the preferred methods of attack by many hackers.

Now, “white hats” can duplicate some types of methods of SQL injection by trying to find vulnerabilities. One of the tools available to a white hat running the Kali Linux distribution is “metasploitable”, a virtual linux machine that will allow a person to practice gaining access and looking for vulnerabilities using the SQL injection method.

The “metasploitable” virtual machine is available online, or may even be contained in the bundle or installation of your Kali Linux. It should include various duplicates of web applications that have vulnerabilities, something that will help the “white hat” learn how to find vulnerabilities and how access to them is gained, which in turn can help the network security professionals find a way to shore up those vulnerabilities by patching them out or developing workarounds.

After installing or opening the “metasploitable” virtual Linux machine, the user can login, with the default username and password of the application being set to “msfadmin”. Once logged in, the user should change the application’s network settings to “bridge”, and restart the machine in order to make sure that the changes have properly taken effect.

CHAPTER 6) QNA ON HOW TO HACKING WITH KALI LINUX

QUIZ

1. What is Keylogger?

2. What is Denial of Service (DoS/DDoS)?

3. What is Vulnerability Scanner?

4. What is Brute Force Attack?

5. What is Waterhole Attacks?

6. What is False WAP?

7. What is Phishing?

8. What is Clickjacking Attacks?

9. What is Bait and Switch?

10. What is Social Engineering?

11. What is Rootkit?

12. What is Packet Analyser?

13. What is Name-dropping?

ANSWERS

1. A keylogger is a very simple piece of software that is designed to track and record each keystroke made by the user of computer. These keystrokes and sequences are then stored on a log file that is accessed by the hacker who is able to discern your information such as email ID's, passwords, banking details, credit card numbers and virtually anything else that you input into your machine using the keyboard. For this reason, many online banking sites and other highly secure web pages use virtual keyboards and even image identifying passcodes to provide you with access to your account since these cannot be recorded through keyloggers.

2. One of the most common forms of hacking attacks is the Denial of Service, as we had mentioned earlier. This involves causing a website to

become unusable. The site is taken down due to the flooding of information and traffic, enough to overload the system as it struggles to process all the requests and is ultimately overwhelmed and crashes. These attacks are employed by hackers who aim to disrupt websites or servers that they want to cause destruction to for whatever their reason or motivation was.

3. To detect weaknesses within a computer network, hackers use a tool known as vulnerability scanner. This could also refer to port scanners which are used to scan a specific computer for available access points that the hacker would be able to take advantage of. The port scanner is also able to determine what programs or processes are running on that particular port which allows hackers to gain other useful information. Firewalls have been created to prevent unauthorised access to these ports however this is more of a harm reduction strategy rather than a sure-fire way to prevent hackers.

4. If you have ever wondered why you have a limited number chances to enter your password before being denied access, the server you are attempting to access has a safeguard against brute force attack. Brute force attack involves software that attempts to recreate the password by scanning through a dictionary or random word generator in an extremely short amount of time to hit on the password and gain access. For this reason, passwords have advanced to become far longer and more complex than they once were in the past, such as including characters, numbers, upper and lower-case letters and some going as far as barring words that are found in the dictionary.

5. Waterhole attacks are known by this name due to the fact hackers prey on physical locations where a high number of people will access their computers and exchange secure information. Similar in a way that a waterhole can be poisoned for the wildlife surrounding, the hacker can poison a physical access point to claim a victim. For example, a hacker may use a physical point such as a coffee shop, coworking space or a public Wi-Fi access point. These hackers are then able to track your activity, websites frequented and the times that you will be accessing your information and strategically redirect your path to a false webpage that allows the information to be sent through to the hacker and allow them to use it at a later time at their leisure. Be sure that when you are using public

Wi-Fi, you have appropriate anti spyware and antivirus software to alert you when there may be suspicious activity while online.

6. Similarly, to the waterhole attack, the hacker can create, using software, a fake wireless access point. The WAP is connected to the official public wireless access point however once the victim connects they are exposed and vulnerable in that their data can be accessed at any point and stolen. When in public spaces, ensure that the WAP you are using is the correct one, they will generally have a password prior to access or a portal which will require you to enter a username, email address and password which is obtained from the administer. If you find the access point is completely open, this could be a cause for alarm knowing that this point is likely bait.

7. Another common technique used by hackers to obtain secure information from an unsuspecting victim is through phishing. Phishing involves a hacker creating a link that you would normally associate with a site that you commonly access such as a banking site or payment portal. However, when you input your details, they are sent to the hacker rather than the institution that you you believe you are sending them to. Phishing is often times done through sending false emails that appear as though they are from your bank or billing institution and generally request that you access your account to either update your details or make a payment.

8. If you have ever attempted to stream a video on a less reputable site, you may have noticed that the interface can be quite confusing to navigate due to false play buttons or common sections after which you click on them and are then redirected somewhere else. These are known as Clickjacking attacks as well as UI Redress. While redirecting to the ad or another page may seem harmless, when done correctly these attacks can be quite sinister and potentially dangerous as they are able to capture your information. You need to exercise extra caution when using unfamiliar websites as they may not be as safe as they appear, with their interface taking you to a place right where the hacker wants you. Always be aware of the URL of each click you make and if it differs drastically from the website that you were just on, ensure that where you are taken does not involve any downloads or exchanging of details for your own protection.

9. The bait and switch technique involves the hacker supplying you with a program that appears to be authentic but when it faces it is a virus or a tool

used by the hacker to access your computer. These can generally be found in unscrupulous websites that offer pirated programs, software, movies or games that are in high demand. Once you download the program, you will find that the file is not what you had intended and instead had loaded a virus to your computer to provide the hacker with access.

10. We mentioned earlier, the social engineering techniques used by white hat hackers. This technique is often overlooked as a means of hacking however it can be quite effective. An example of social engineering is conning a system administrator into supplying details by posing as a user or an individual with legitimate access. These hackers are often thought of as con men rather than what we understand to be hackers, however it is a means of hacking nonetheless. Many of these hackers have a good understanding of the security practices of the organization in which they are attacking.

11. A rootkit finds its way onto your operating system through legitimate processes, using low-level and hard to detect program. The rootkit can assume control of the operating system from the user and since the program itself is hidden within the system binaries as replacement pieces of code, it can be incredibly difficult and virtually impossible for the user to detect and remove the program manually.

12. When transmitting data across the internet or any other network, an application known as a packet analyser or packet sniffer can be used by a hacker to capture data packets which may contain critical information such as passwords and other records.

13. Having the name of an authorised user provides the hacker with the advantage that they can pretend to be a specific person who should rightly have access to the information. This can be done by sourcing through web pages of companies which can be easily found online. Another example of this is the searching through documents that have been improperly discarded, providing vital details to the hacker.

CHAPTER 7) PROCESS MANAGEMENT

i. METHODOLOGIES TO KILL A PROCESS

The first step is to find a wireless network to hack: remember that “just trying” or “I’m learning” is not an excuse, and any unauthorized access or attempt to access without authorization may be punishable, so best that you ask permission, or better yet, simply create your own wireless network for convenience.

Now that we have a wireless network to work with, the next step is to find out the name of your own device’s wireless adapter. Note that there are a couple of terms that we should be familiar with: “eth – ethernet”, and “wlan – wireless local area network”. The “wlan” is what we’re looking for, so keep an eye out for that. Boot up your Kali Linux terminal and type in ifconfig, which should show us a lsit of all the terminals of our computer. Take note of the “wlan” adapter, along with the suffix, which is usually 0 / 1 / 2.

Now that we have our wireless adapter, we now have to enable monitor mode. The user can employ a tool called airmon – ng to create a “mon” virtual interface. This can easily be done by typing

Airmon – ng start wlan0

This should create a monitoring interface, which would be named by default as - mon0 if using an earlier version of Kali Linux, but if using the Kali Linux 2.x onwards, the name would be wlan0mon.

Once the monitoring interface is up, we can begin to attempt to capture data packets that are being transmitted by the wireless network that we are trying to crack into. The following tool should help us gather data:

Airodump – ng wlan0mon

That should allow us to access a few data packets. If we want to save the data in a file, which we do, we add another command to the end, “write *filename*”, so it should look like the following:

Airodump – ng wlan0mon - - write *filename*

That will store any captured packets in *filename*.cap. Once we have about ten thousand data packets minimum stored, we can proceed with the wifi cracking process.

One of the more common attacks, as earlier discussed, is SQL injection in order to gain access to a website or a database. Though the reader should know this by now, just for review: SQL is a structured query language that allows the computer to manage data, in order to store, manipulate, and retrieve data from the server or system database. The database is the repository of all the data, often containing passwords and other sensitive information.

So what is SQL injection? SQL injection is a way of injecting queries into the database. Now the database is specifically meant to answer queries, but only from authorized sources. SQL injection is a method wherein external queries, from unauthorized sources are granted access to the database. This is done through “inserting” them into the normal flow of data queries in order to disguise them as authorized requests for information. This allows the hacker to retrieve the information in the database, whether it be passwords, encryption keys, or even raw data. There are also some SQL injection methods that not only allow for retrieval of information, but even insertion of malware or other files, which may allow the hacker in question to control the database, either locking out the owner or even deleting some or all the files within. Needless to say, SQL injection is one of the preferred methods of attack by many hackers.

Now, “white hats” can duplicate some types of methods of SQL injection by trying to find vulnerabilities. One of the tools available to a white hat running the Kali Linux distribution is “metasploitable”, a virtual linux machine that will allow a person to practice gaining access and looking for vulnerabilities using the SQL injection method.

The “metasploitable” virtual machine is available online, or may even be contained in the bundle or installation of your Kali Linux. It should include various duplicates of web applications that have vulnerabilities, something that will help the “white hat” learn how to find vulnerabilities and how access to them is gained, which in turn can help the network security professionals find a way to shore up those vulnerabilities by patching them out or developing workarounds.

After installing or opening the “metasploitable” virtual Linux machine, the user can login, with the default username and password of the application being set to “msfadmin”. Once logged in, the user should change the application’s network settings to “bridge”, and restart the machine in order to make sure that the changes have properly taken effect.

ii. PRIORITISINNG PROCESSESES

The hacker now has access to the resources available on the database of the organization. The hacker is then free to either extract the information that he sees of value or he is able to take control of the network and use it as a base to launch further attacks against other targeted networks in how we described a DoS attack. By gaining access to the network, the hacker now has control over one or more devices.

As was the case in the preventative measures of scanning, there are some precautions that administrators and security personnel are able to take to ensure that devices and services are more challenging to access by legitimate users such as black hat hackers. This can involve restricting access of users such who have no legitimate day to day requirement to be accessing the devices. Furthermore, security managers should be closely monitoring the domains and those who are accessing services such as local administrators. Using physical security controls will allow managers to detect attacks that are occurring in real time and can deny access while also alerting the proper authorities to ensure the intruder is exposed.

Another approach which can be taken to ensure that access is denied is to encrypt highly sensitive and confidential information using protection keys. This would mean that any attacker attempting to access the system regardless of how well the system is protected, will gain access only to find that the information is scrambled and with the keys protected, the attacker would have no reliable method for using the data that has been encrypted. Encryption is a good final line of defence for particularly valuable data however it cannot be relied upon entirely in itself. Even if the attacker was to access the system and discover that the data is encrypted, they can still wreak havoc on the network and even disable it, causing significant damage as a means of sabotage. Even more alarming,

the attacker could have control over the system and use it for further crimes which could be traced back to the organization's network.

Once the attack has gained access to the system, they are still far from being in the clear. Access is for a limited time, the longer the hacker is operating from the system, the greater the chances of being caught. The hacker must then shift to the next phase, maintaining access to ensure they are able to collect as much data as possible.

Maintaining Access

The hacker is working against the clock at this point and they must ensure they are able to maintain access long enough to succeed in what they had set out to do whether this was to steal critical data and information or to launch a further attack from the encumbered server. The hacker has been able to avoid detection up until this point, however they are still at risk of being caught and the longer they have access to the system, the higher the risk they could be detected.

Covering Tracks

You are aware that there are a number of attacks launched using the network, which means that hackers do consider access points to be among the most vulnerable aspects of any information technology fortress. If you remember the Heartbleed incident, you would realize that even top corporations can be easily exploited over the network, even causing their more advanced systems to suddenly spit out confidential and encrypted information about their clients. If they are vulnerable, then so are you.

If you suspect that your system has been attacked over your network, or that someone has made an announcement that they are going to hack you, then you have all the right reasons to monitor what is going on in your network and try to find out who your attacker might be.

CHAPTER 8) WORKBOOK

QUIZ

1. What is free – use software?
2. What is Open Source Git Tree?
3. What is File System Hierarchy – standard – compliant?
4. What is Support for a wide variety of devices?
5. What is Custom Kernel?
6. What is Secure Development Environment?
7. What is Multi – lingual support?

ANSWERS

1. Much like the predecessor, BackTrack, Kali Linux is available for use free of charge, and according to the developers, they intend to keep it that way, making this tool available for download and use without need for any paywall, with all users receiving full functionality of the Kali Linux distribution.
2. Kali Linux is freeware, and much like other freeware and many Linux distributions, it is also open source. The developers of Kali Linux are committed to using the open source development model, allowing their development tree to be made public. In addition, all the source code used in Kali Linux is also consistently made available by the developers, for any user that wants to tweak or modify Kali Linux for a specific need.
3. The Kali Linux software is adherent to the FHS, or the "Filesystem Hierarchy Standard", making it much easier for Linux users to navigate and locate specific files such as binary codes, support files, software libraries, and the like. The use of this standard allows for convenience and ease of

use, one advantage that Kali Linux has over a lot of other similar software.

4. The developers of Kali Linux have tried their best to make Kali Linux as user – friendly and versatile as possible, making it compatible with a large range of platforms. Kali Linux is supported by multiple operating systems, and one of the biggest things is that Kali Linux itself supports the use of wireless devices. Not only is Kali Linux compatible with multiple software setups, but also a large range of hardware setups, and the developers are trying their best to include as many hardware configurations as possible. This is quite notable, especially due to the wireless device support, as one of the regular criticisms against most Linux distributions is that they tend to lack support for wireless hardware, which Kali Linux provides.

5. Kali Linux's development team are, first and foremost, penetration testers, meaning that they are often required to do assessments wirelessly, and as such, the kernel of Kali Linux has injection patches constantly included, keeping it up to date.

6. The Kali Linux team is made up of "white hat" hackers and penetration testers, and as such, they are acutely aware of the need of security, especially when it comes to software that "white hats" often use, as a vulnerability or bug in the software itself can have disastrous and wide – ranging results. As such, the development team is restricted, and they are the only ones who commit packages and interact with Kali Linux's repositories, all of this being done under multiple secure protocols to ensure fidelity and security. In addition, Kali Linux's packages and repositories are GPG signed, with all packages contained by Kali Linux signed by the individual developer responsible for building and committing it, and each repository also signs the package, allowing for a secure set of software packages and repositories.

7. Though much of coding and a lot of penetration tools are built on the English language, Kali Linux attempts to include multi – lingual support, allowing non – native English speakers to operate in their native language, making it easier for them to make use of Kali Linux and its features, enabling them to be more effective in carrying out their tasks.

CONCLUSION

We have come to the end of this book. Kali Linux is a very powerful Linux distribution, especially for penetration testing. The OS comes with a number of tools which can help you do penetration testing on systems and applications. This makes Kali Linux the best operating system to use for penetration testing. Before deploying your system in a working or production environment, it is good for you to first test it via penetration testing so that you can be sure that it has no loopholes. With penetration testing, you can identify the loopholes in your system and seal them before using it for production. This will help you prevent disasters which might have occurred as a result of exploitation by hackers.