HACKING

Learn the Basics of Ethical Hacking and Penetration Testing

MARTIN DONOVAN

Hacking

Learn the Basics of Ethical Hacking and Penetration Testing

Table of Contents

Copyright Notice

Disclaimer While all attempts have been made to verify the information provided in this book, the author does not assume any responsibility for errors, omissions, or contrary interpretations of the subject matter contained within. **The information provided in this book is for educational and entertainment purposes only. The reader is responsible for his or her own actions and the author does not accept any responsibilities for any liabilities or damages, real or perceived, resulting from the use of this information.**

Introduction

Ethical hacking is a way to turn your mischievous thoughts into legal work that pays quite well. Businesses will pay you generously to do what malicious hackers want to do – to access their systems and steal valuable information. You won't steal the information, however. When you find vulnerabilities, you will report them to the IT departments of the companies for which you work, so that they can repair the problems.

Ethical hacking, also known as white hat hacking, is a way for organizations to ensure that they are compliant with government and corporate mandates, to keep customers' information safe and private. You'll learn all the tools of the hacking trade, both automatic and dynamic, so that you can keep your employers as safe as they possibly can be against hacker attacks and information breaches.

BONUS: Your FREE Gift

Thank you for purchasing my book: "*Hacking*". I want to show you my appreciation by offering an exclusive Special Report "*TOP 10 Gadgets Of The Year*" for FREE.

Simply Click the Button Below

Click Here to Download the ebook

OR Go to This Page

http://bit.ly/1AiwLLM

Chapter 1 – What is Ethical Hacking?

Computer hacking can occur in many ways. The intent may be malicious or benign. Benign hacking by workers in the security industry is called ethical hacking, which describes attacking a public or private network or system benevolently, to check on the security of the system or network for its owners. Ethical hackers may sometimes be referred to as white hat hackers. This distinguishes them from people who hack into systems with the intent of harm or exploitation. Those are black hat hackers.

One not-so-clear part of hacking is known as hacktivism. In these cases, a hacker will detect and report on security vulnerabilities, but may also exploit them for social activism. In cases like these, sometimes called gray hat hacking, the hacker may not be motivated by money, but rather the goal of calling attention to injustices or issues that the hacker feels merit social change. The victim may not be as receptive of the message.

True ethical hacking should be done with the consent of the organization being targeted, even though some black hat hackers may claim to be working as ethical hackers if they are caught.

Why do Companies Use Ethical Hackers?

Why would someone pay a hacker to attack their own website or application? The reason is to expose any vulnerability they may have. Anyone in law

enforcement knows that in order to prevent criminal activity, it’s best to think like criminals do. Ethical hackers who test security systems use methods just like illegal hackers do, but instead of disrupting the company, they report any problems they find.

The Federal government utilizes many ethical hackers. Larger companies employ entire teams of white hat hackers as part of their plans for information security. If you are tech savvy, or a computer programmer, you can take classes that will help you learn ethical hacking, and you can even be certified in the skills.

Application testing utilizes ethical hackers who try to compromise an app and then report their findings. Various tests are performed, including information gathering attempts, all the way up to outright attacks that would damage a company or agency if they were done maliciously. Ethical hacks may include techniques like emailing company staff to see if they will reveal their passwords or other details of their accounts.

Ethical Hacking Tools

Ethical hackers use tools that expose vulnerabilities like software coding errors that are threatening to accounts, critical data and the functionality of the applications. Some of this hacking is done manually and some is done with automated tools, like dynamic and static analysis. These will find insufficient encryption or malicious code that could allow security breaches. Ethical hackers can spend time prioritizing problems and remediating them.

Companies find Ethical Hackers Valuable

Large companies have used ethical hackers for many years to test their internal and external security. They are especially valuable in checking new systems being launched. Beyond their testing, they can find overlooked vulnerabilities that could bring damage to the company.

Businesses hire white hat hackers, never black hat hackers. Black hat hackers attacking their systems may very well find vulnerabilities, but they will also take advantage of them.

Most companies find it quite safe to employ white hat hackers, whose skills are used to improve security. They will have the explicit permission of management, and they will test their systems just as if they were malicious hackers. They can perform vulnerability assessments, quantify risks and threats, and disclose their findings so that the problems can be repaired.

If you enter white hat hacking, you will use most of the same tools as malicious black hat hackers do. You will need to train in the area, and keep your knowledge and skills up to date, so that you know the latest exploit possibilities. You do not need to be certified after you train to do white hat hacking, but it will put company managers at ease when they hire you.

Early Discovery of Security Issues is Essential for Business

Some major vulnerabilities are discovered before they can be exploited. Security team members work diligently to rid their system of flaws before a black hat hacker finds them.

Well-intentioned ethical hackers work together with business management to probe networks for holes in their security systems. They use the mindset of a black hat hacker who has criminal motivations.

Companies hire ethical hackers or retain them on staff to determine how real criminals would attack their system. They know all types of tricks that will allow them to sneak in. Some of them include:

- Hacking their way in
- Conning employees through email or on the phone
- Using false paperwork to walk right in

Any business can be compromised on some level. From hospitals to banks and even Fortune 500 companies and government agencies, everyone is vulnerable.

Is Ethical Hacking a Full Time Job?

White hat hacking can be a full time source of income, and the work is challenging and interesting. It rewards you, since you're protecting companies from malicious black hat hackers who could otherwise break into a system.

Most ethical hackers have worked with computers for some time. They value persistence and hard work and they set their own goals. They may enjoy teaching non-damaging tricks in schools and eventually settle into companies or

freelance arrangements to help people and companies with computer security.

An interest in and skills with computers give you great potential to be a white hat hacker. You'll learn not to allow obstacles to rattle you, but instead to use logic and technology to overcome issues. If you enjoy working in the field of technology, you can actually do good work, and that's a rewarding experience.

Who can become an Ethical Hacker?

Many people have been drawn to white hat hacking. They come from all background types and with various motivations. Basically, if you're drawn to intricate technology and you enjoy the challenge of bypassing problems, you can make it a career.

How do you get a Job in Ethical Hacking?

White hat hacking isn't a "normal" job. You don't need a college diploma to do it. You just need a familiarity with computers, programming languages and software. You must be creative and driven.

Many people who worked in IT jobs until the dotcom bubble burst have found a new career in ethical hacking. To keep criminals out of the company for which you work, you must learn how they operate – their tricks. Taking ethical hacking courses will give you more specific skills.

Are Certifications or Licenses Required?

You do not need certification to work as an ethical hacker, but you will find more companies willing to hire you if you are certified. It proves your experience, your knowledge and your good intent. The type of certification you choose will depend on the type of business you will be working with. Research any classes or certifications before you sign up.

There is one exception to not needing a license for white hat hacking. If you perform investigations for your clients, your state will probably require that you hold a private investigator license. As long as you have good communication skills, persistence, problem solving abilities and are skilled in the field, you can be a competent ethical hacker.

Chapter 2 – What will you do as an Ethical Hacker?

White hat hackers go inside company networks in major companies like utilities, hospitals and banks, to see how vulnerable their systems are if an attacker targeted them. You may find some important systems being run on older hardware and software. A company may have un-patched programs that leave them vulnerable, or old default passwords that have never been changed.

The network of business computers, which you count on to protect your records and keep your utilities on, is actually a patchwork of systems with problems that are much easier to exploit than you might like to think.

Catching Attacks before they hit the News

Much of the time in an ethical hacker's day is spent scanning or probing networks, seeking vulnerabilities. You will also need to communicate effectively with clients and document what you have found and what you have done. The final report is something your clients will keep and ponder over long after your job is done.

Clients can see most of what you do as an ethical hacker. The process is open, and they may learn from your perspectives about their network.

People have Misconceptions about your Job

Most people, when they hear the term “hacker”, immediately think of a malicious hacker, or a criminal. Hackers like to tinker with software and tools, and learn new means of problem solving. They can open up new ways to use existing technology. Hackers who steal are criminals. Ethical hackers do not associate themselves with criminal hackers.

The managers for whom you work will also feel like your simulated attacks are magic. You will learn that computers just do what you tell them to, and sometimes those actions are not in the best interest of company management. They may run software that is not properly coded or click on a spam email that promises them money. Most users are not aware of the scary, dangerous things they can do to their system.

Business owners also may have a lack of knowledge about what ethical hacking will include. They are learning more today to pay ethical hackers before black hat hackers attack their systems, though.

How long do Ethical Hackers Work on a Project?

This is dependent on what you are performing. If you are hired to check for all types of penetration issues, you may work between eight and 10 hours a day. The project may run between two weeks and two months, or even longer. You may find, as many white hat hackers do, that they have to remind themselves when to go home for the day, since the work is challenging and interesting.

If a company calls you in after their security has been breached, this is known as crisis mode or incident response work. You may be working day and night to help in controlling the damage and helping to get the business back on its feet.

Are there different Levels of Ethical Hacking?

Some companies only scan a system for vulnerabilities and that's all. There is a problem here. They're not telling the company owners about which programs are vulnerable and how attackers would work to take advantage of the vulnerability. How much damage could be done?

Most white hat hackers are very goal-oriented. They feel that their work helps companies understand real world consequences for any vulnerability in their system. What would attackers do with the information they find? Would they steal data, interfere with computer programs or perform wire transfers of cash?

When ethical hackers find network vulnerabilities, they also check for practical consequences of those shortcomings. Creativity is needed to understand a security flaw's full potential. You must be able to put the pieces together and figure out the ways in which criminals could pull off a financial or data heist.

Does the Work cause any Frustration or Stress?

It can be frustrating when clients prefer not to know they are vulnerable. They may believe that it will be cheaper to fix a problem after they are breached than to spend money on better security before they are hacked. Usually their delay is

based on fear.

You know how your car begins making funny noises but you turn the radio up because the repairs could be costly? That's how many businesses deal with potential security threats. In addition, senior IT executives may be worried about how problems will make them look, and they are worried about their career.

To deal with these companies, do your absolute best, and report clearly where they are most vulnerable, and what it means for them. If business executives are not sure about taking the necessary steps to protect their companies and their customers, you just will hope they will do the right thing.

What do Ethical Hackers Enjoy about their Jobs?

Most white hat hackers become excited about knowing their job would be illegal except for the contracts with companies that allow them to hack with permission. Some of these people think like criminals, and that's really what you need to do, in order to find areas where companies are most vulnerable.

You will work with some amazing people, and the work is hard but fun. You'll learn together. You will be making a difference in the mindset of companies and their security, and you will also save thousands of customers money and hassle. You may be surprised at how good the pay is, too.

How would you Advise Companies who are thinking of Using your Service?

You must make it clear to company executives that you are not a superhero. Some clients will believe that once they hire you, everything will be cleaned up, every problem will be fixed and they will be 100% secure.

In today's world of malicious hackers, there are no 100% secure companies or systems. The realistic goal is figuring out what assets are the most critical to them and what types of risks they are willing to accept. No one can prevent every possible attack, even if you're an excellent ethical hacker. Eventually, someone will figure out a way to get through the defenses. You will not only be preventing attacks, but also you'll figure out the steps that can be taken to limit damage in the case of any successful attack.

To do the best job possible, you need to know all of the company's information, systems and risk assessment documents that have looked at the overall risks of the company. These are important tools you'll need to do your job effectively.

Testing a client's systems has a goal of finding weakness, then exploiting it, which shows how an unacceptable, critical risk can be realized. This includes removing sensitive information from their network and placing it on your secure network. In this way, you can better expect to remediate company risks. The most difficult work for your client will come after you have tested their systems, and teach them to do their business in a way that is less risky.

Do Ethical Hackers Make good Money?

If you do your job well and hone your skills, you can make good money working as a white hat hacker. Freelancers may not make as much as hackers who work for one company. However, if one company employees you, then they “own” you. They can force you to travel and they won’t worry about your lack of time to sleep.

If you want to balance life and work, you’ll first need to have experience in conventional IT work and in the field of security, before you’ll make big bucks. Your location will also affect how much you make. Areas with higher costs of living usually have higher pay.

Can a person move up and advance as an Ethical Hacker?

This is a subjective question. Some hackers will specialize in key areas, including:

- Industrial control systems (manufacturing plants, utilities, etc)
- Software security (web and mobile apps)
- Social engineering (hacking individual people)
- Management skills (running teams of white hat hackers)

In all of these scenarios, you must focus on increasing your knowledge of the field and gaining as much experience as you can. Certifications will help, but nothing replaces experience.

You can also make yourself stand out to potential clients by conducting your

own research into the largest security issues and presenting them at industry conferences. Running training camps at conferences to teach key security skills is also advantageous.

What do Hackers' Clients overvalue or undervalue?

Your clients will generally undervalue their role in the security process. They think that if they have hired you, that you'll keep all the bad guys out. They usually undervalue their assets, too. Some small companies have the mistaken belief that they are not large enough to be of worth to malicious hackers. Many executives think it won't happen to them until it does.

Executives also compare their companies to others in their area or type of operation, which is a mistake. They don't want to spend more on their security than others in their area, or they think it's money wasted.

Company management may also undervalue compliance standards. This could be HIPAA for healthcare companies or PCI for retail companies. Meeting a standard of compliance does not make a business secure. Compliance standards are simply the baseline of what companies have to do if they don't want to be fined. To be as secure as they can possibly be, they must go much further.

Chapter 3 – Learning to become an Ethical Hacker

There are various companies that offer courses in ethical hacking. The basic courses last five days or so and will certify you under Certified Ethical Hacker (CEH) certification, the standard for ethical hacking certification.

The best courses on information security and ethical hacking will cover the methods used by malicious hackers, and you will have lectures to attend, along with lab exercises to give you hands-on experience. The classes teach you the same skills that are used for malicious hacking, and how to use them in performing white hat ethical hacks for the companies for which you work.

You will finish these classes with an ability to assess and accurately measure threats to most information assets. You will also have the skills to discover where your employers are most vulnerable to black hat hacking. The course goals are to assist you in mastering a documentable, repeatable method for hacking systems to use in white hat hacking situations.

Black hat hackers constantly change their tactics to stay one step ahead of you. Courses in ethical hacking update course materials on a regular basis, so that you will learn more about the current threats to your employers' systems and networks.

Course Teachers are Experts in Information Security

The instructors in the best CEH courses have experience in the industry and are recognized experts. The course you choose should have a high percentage of passing students, who are certified in the latest levels of CEH.

What do you learn in Ethical Hacking Courses?

In the best classes, you will learn how to run hack attacks in the labs, and become hackers for a week while still in training. Some of the most important skills you learn include:

- Stealthy network reconnaissance
- Penetration testing methods
- Exploiting remote root vulnerability
- Passive identification of online traffic
- Remote access Trojan hacks
- Privilege escalation hacking
- Running shellcode in RAM and on disc
- Abusing Windows pipes for impersonation
- Wireless insecurity
- Removing evidence
- Anti-forensics
- Brute force hacking
- Network infrastructure hacking
- Hacking web apps
- Breaking into unsecure databases
- Defensive techniques

What will you do in class?

Instructors lead hands-on lab exercises in hacking in:

- Abusing DNS for host identification
- Capturing the flag hacking
- Windows cache poisoning
- Leaking system information
- Password cracking on Cisco and Windows
- Stack versus heap overflows
- Impersonating other system users
- Attacking remote desktop protocol in Windows
- Data mining
- Remote keylogging
- Hijacking SSL encrypted sessions
- Calculating Return on Investment for ethical hacks

Compliance and Certification

In any ethical hacking course, you need to be afforded the chance to prove to potential employers that you can use the skills in which you are certified. Good courses will prepare you fully for passing the latest CEH certification tests. They go beyond CEH material as well, to give you more exposure to white hat hacking.

What must you know before you attend CEH Courses?

Before you spend the time and money to take certification testing, course work will teach you an understanding of Windows OS, Linux or Unix-based OS. You should understand IP protocols and have a desire to learn more about network security.

Look for courses with smaller class sizes (usually between 10 and 20 students), so that you'll have more one on one time with expert instructors.

Choose courses with exemplary records and full-day training sessions.

Some courses include the exam fees for the CEH examination.

Hacking lectures are often available online in addition to in-person. This allows you to go back to information you may not have retained in class, since so much information is presented.

The best courses are built on a commitment to ongoing education for ethical hackers. Some courses offer a research and development site, where they post articles, labs, tutorials and white papers that will help in your continuing CEH training. Forensics videos are often available.

Some of the skills you learn will include:

Hacker Tool Kit

This is a set of hacker tools placed on compromised systems so that you can learn how to attack the systems or escalate privileges. The kit itself generally contains a tool for creating back doors and listeners, and a port scanner. It will also include other tools used during the course for discovery and exploitation of weaknesses.

Creating Host System Directories

You will learn to create directories disguised by names that won't alter system administrators or general users. You will also be taught to stream or hide files to avoid detection.

When you have access as an administrator on a compromised host, you will be able to run your tools remotely from that host, or use it to redirect ports. This involves taking traffic from one network on one port and redirecting it out from the host of another port.

Holes in Applications

These are general categories that refer to specific oversights or programming errors that will allow you to penetrate business systems. You will conduct penetration testing to identify the apps running on a remote system. Once you identify them, you can look for exploits and vulnerabilities that will affect the apps. You can often capture an app banner, to perform the app identification.

In searching the Web and databases for exploits, you may find processes or exploits that will lead to a compromised system. You will be taught to gain access, where possible, to systems in a business demilitarized zone (DMZ) to identify versions and apps run on that system. You will research vulnerabilities in management services that will enable you to capture SAM files from the repair directory on a system.

Testing outside Firewalls

On testing systems outside firewalls, you can make a connection to the Web with a different port not filtered by that firewall. Then a listener can be established and the connection can be redirected. Using this type of port redirection, you will be able to bypass filter rules on routers. You can also use a remote compromised host to test the advantages of trust relationships.

Buffer Overflow Attacks

These are also known as data-driven attacks, and you can run them remotely to escalate privileges and gain local access. Buffer overflows are generally designed for UNIX, since OS knowledge is needed when writing a buffer overflow. Windows also has buffer overflows, but they are more commonly found in a UNIX environment.

Where source code is available, you can study and learn what you need to create the buffer overflows for UNIX. These attacks attempt to force target hosts to

change execution flow and execute the code you specify, as the attacker. You can do this by forcing the designated target to place too much data into a target buffer with a finite capacity. This creates the overflow.

This will usually crash or stall the application through which data is loaded. Buffer overflow training usually only needs to be downloaded onto a target system before it is compiled and then executed. You won't always need root privileges to run them successfully. The most difficult part of these tasks is finding an overflow that will work on your specifically chosen target.

Buffer overflow attacks are effective and dangerous. If you launch an attack of this type against a target that is susceptible, you may need to tweak it, but it will usually work. Use them only when you know what they will do, and what the consequences might be. In addition, experiment only on your own machines. These overflows may cause system crashes, which leads to the condition of denial-of-service. Be sure to get written permission from clients before you run buffer overflows on their systems.

Chapter 4 – What is Penetration Testing?

Penetration testing involves an authorized and proactive evaluation of IT infrastructure security by using hacking methods to exploit any vulnerability in the system. These include risky behavior by end-users , improper configurations, applicant and service flaws and Operating System problems. These assessments will also validate the success of defense mechanisms and the way company users adhere – or do not adhere – to security policies put into place by their employers.

These tests are usually done with automated or manual technologies that compromise mobile and network devices, wireless networks, web applications, endpoints, servers and other exposure points. Once any vulnerabilities are exploited on a system, the testers may try to utilize the now-compromised system to achieve higher security resource levels and more intimate access to information and electronic assets via the escalation of privileges. Ethical hackers are often called upon to conduct penetration testing.

Security vulnerability information that is exploited successfully through penetration testing will usually be gathered and presented to the network systems and IT managers. This will assist them in making strategic conclusions and prioritizing related efforts at remediation. The main purpose of this type of testing is measuring the feasibility of systems and evaluating any consequences that these incidents could have on operations and resources.

Why should your Company have Penetration Testing Performed?

Service interruptions and security breaches cost companies big money. Interruptions in performance of apps may result in losses financially, and threaten the company reputations by eroding customer confidence. They can also trigger penalties and fines and attract negative media coverage.

The average total cost for companies with data breaches averages a staggering $3.5 million. For larger breaches like the 2013 Target data breach, though, the costs can be higher – theirs have already gone over $148 million.

No one can protect a Company 100% of the Time

Many businesses have tried to prevent breaches through the installation and maintenance of defensive security layers. They include firewalls, cryptography and user access controls. However, new technology and its complexity make it more difficult to protect a system against security problems and to eliminate all vulnerability. Newer vulnerabilities are being discovered nearly every day, and this means that attacks are constantly evolving in their social and technical sophistication.

Identifying and Prioritizing Security Risks

Penetration testing will evaluate a company’s abilities in protecting their users, applications and networks from internal or external attempts to get around security controls with the purpose of gaining privileged or unauthorized access to their protected assets.

This type of testing will provide validation that there are risks posed by flawed processes and security vulnerabilities. This allows security and IT management professionals to more easily prioritize their efforts at remediation. By using more comprehensive and frequent testing, companies can anticipate risks more effectively and be more likely to be able to prevent any unauthorized access to valuable information and critical systems.

How often is Penetration Testing Performed?

This type of testing needs to be done frequently, if companies hope to ensure security that is more consistent with threats. There are always new threats that can be capitalized on by black hat, malicious hackers. Companies should also run tests each time:

- Policies for end users are modified
- Security patches have been applied
- New locations are opened
- Significant modifications or upgrades have been applied
- New applications or network infrastructure is added

How can Penetration Testing Benefit a Company?

This type of testing provides businesses with multiple benefits, which allows them to manage vulnerabilities. Detailed information provided on exploitable threats in security through penetration testing proactively identifies the most critical vulnerabilities. With this information, a company can apply security

patches where needed and allocate their resources efficiently.

Penetration testing helps businesses to avoid fines and meet regulatory requirements. An organization can be helped in addressing the compliance and auditing aspects of their business. It can specifically address requirements documented within federal mandates. Testing results are given in report form to help companies learn the best ways to avoid fines and perform due diligence by maintaining proper security controls.

Recovering from security breaches is expensive, and can cause network downtime. Customer retention and protection and IT remediation, along with legal work, can reduce the company's revenue. When a business proactively identifies risks before breaches or attacks occur, they will avoid the financial pitfalls.

Preserving customer loyalty and a good corporate image are vital to any business. Even one compromised data incident can cost a great deal in lower sales and in loss of a positive image. No business wants to lose customers that they have always worked hard to keep.

Penetration Testing versus Vulnerability Scanning

Company executives are sometimes confused by the difference between penetration testing and vulnerability scanning. They don't have the same meaning. Vulnerability assessments only identify and report vulnerabilities. Penetrating testing exploits vulnerabilities, if possible, to see whether malicious

attacks are possible.

Penetration Testing Tools

These are used as an integral part of penetration testing. They will automate some tasks, improve the efficiency of testing and allow for the discovery of issues that may be hard to find if you're only using manual techniques.

Ethical hackers may use dynamic or static analysis tools. They both will help in finding vulnerabilities in security like malicious code and problems in functionality. These tools help you in determining whether the encryption used is sufficient or whether a software component contains back doors through which malicious hackers could gain access.

Manual Penetration Testing

This testing includes professional tools and software along with human expertise.

Manual penetration testing layers human expertise on top of professional penetration testing software and tools, such as automated binary static and automated dynamic analysis, when assessing high assurance applications. A manual penetration test provides complete coverage for standard vulnerability classes, as well as other design, business logic and compound flaw risks that can only be detected through manual testing.

Penetration testing is one vital method by which you will be able to help organizations maintain their security, after you have been trained as an ethical hacker.

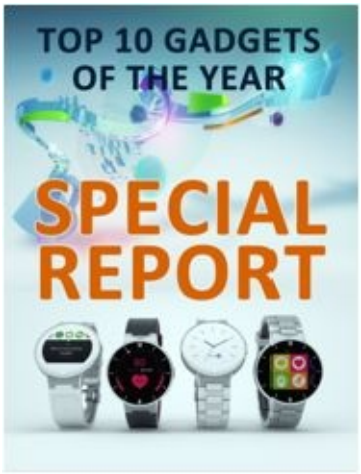
Conclusion

Are you ready to become a white hat hacker yet? We've given you some compelling reasons to choose this job, and helpful information about how to study and become certified in this lucrative field.

To fight back against all the malicious, black hat hackers out there, organizations need ethical hackers to find vulnerabilities in their information systems. Then they can use the information you provide to fix any leaks or malfunctions in their networks, to avoid being attacked by tech-savvy hackers who want to steal information to use for their own purposes.

Ethical hacking is a way to make a living in a challenging and interesting employment field. You may find out that it's quite rewarding to protect organizations and help them to keep their important information safe from black hat hackers.

FREE Bonus Reminder



If you have not grabbed it yet, please go ahead and download your special bonus report "*TOP 10 Gadgets Of The Year*".

Simply Click the Button Below

Click Here to Download the ebook

OR Go to This Page

http://bit.ly/1AiwLLM

BONUS #2: More Free Books

Do you want to receive more Free Books?

We have a mailing list where we send out our new Books when they go free on Kindle. Click on the link below to sign up for Free Book Promotions.

=> Sign Up for Free Book Promotions <=

OR

Go to this URL http://bit.ly/1COlFPe