Chapter 1

An Introduction to Ethical Hacking

This book focuses solely on ethical hacking. It will detail how you can use different techniques to test your system or network for any vulnerabilities and then fix those vulnerabilities before a cracker exploits them. Most people misuse the word “ethical”, often not understanding what it even means. The definition given in the Merriam Webster dictionary suits the purpose of this book. An ethical hacker can perform the different tests mentioned in the book once the system owner gives him or her permission to perform the hack.

How Do Hackers Beget Ethical Hackers?

Everyone has heard about hackers, and many people have even suffered losses because of the actions of a hacker. So, who is a hacker, and why is it important for people to learn more about what a hacker does? The next few sections in the book will help you understand the process of hacking and the different types of hackers in the industry.

Who Is a Hacker?

The word “hacker” can be defined in two ways. A hacker is someone who tinkers with software and electronic systems to understand how they work. They also look for ways to improve the functioning of a network and electronic system. They love the challenge of discovering new ways to make systems work. In recent times, the term “hacker” has taken on a new meaning. Hackers are people who want to break into a system or network for malicious purposes. These hackers are called crackers or criminal hackers. A cracker will only break into a system or network to steal, delete or modify some confidential information, which can lead to huge losses for an organization or individual.

This book will use the terms “hacker” and “ethical hacker”, so it’s important that you understand what each means and that they differ from one another.

A hacker is someone who attacks a system with malicious intent, while an ethical hacker will attack a system to test and fix the vulnerabilities.

An ethical hacker, or a white hat hacker, does not like to be called a hacker because people perceive the word negatively. Crackers claim that they are only helping the system or network owner by hacking it, but that's untrue since they are electronic thieves.

Hackers will always attack a system that they believe they can compromise. Most hackers like to attack a prestigious or well-protected system since it's like a game for them. Also, when a hacker can attack a critical website or database, his or her status will increase in the hacker circle.

What Is Ethical Hacking?

Every system or network must always be updated and patched to protect it from a cracker. An ethical hacker is someone who knows how to protect the system or network. An ethical hacker possesses the mindset, tools and the skills of a hacker, but this type of hacker is trustworthy as they only hack systems to run security tests.

If you perform an ethical hacking test for a customer or want to add a certification to your resume, you can sign up for the ethical hacking certification that is sponsored by the ECCouncil. To learn more about the certification, visit their website www.eccouncil.org/programs/certified-ethical-hacker-ceh/.

Ethical hacking (also called penetration testing or white hat hacking) uses the same tricks, techniques and tools to test the system. The major difference is that ethical hacking is legal. This type of hacking is performed only when the owner grants the hacker permission. As mentioned earlier, ethical hacking helps the system's owner discover the vulnerabilities in the system from a hacker's perspective, helping to improve the system's security. This process is one part of the risk management program, which helps the organization or the system owner enhance the system's security. Ethical hacking backs a vendor's claim that the products being sold by the vendor are legitimate.

If you want to hack your system the way a cracker would, you should know how they think. After all, it's always important for you to be familiar with

your enemy.

Why Should You Hack Your System?

You must remember that the law of averages does not work in favor of security. The number of hackers and the amount of knowledge they have is increasing by the day. If you combine that knowledge with the number of vulnerabilities in the system, there will come a time when every computer system is compromised in one way or another. Protecting your system from a cracker is important. However, this does not mean that you should only look at the general vulnerabilities that people are aware of. Once you know how a cracker works, you will know how vulnerable your system really is.

Ethical hacking helps you identify weak security practices and discover any areas needing attention. Encryption, Virtual Private Networks (VPN) and firewalls can often create a false sense of security. However, these systems only focus on traffic and viruses through a firewall, which does not affect the work of a cracker. If you want to make your systems more secure, you should carry out the attack in the same way a cracker would. This is the only way you can harden the security of your system. If you fail to identify these weaknesses, it's only a matter of time before the system's vulnerabilities will surface.

You should expand your knowledge in the same way a hacker does. You should think like one of them if you want to effectively protect your system. As an ethical hacker, you should understand the activities that a cracker will carry out and then identify ways to end their efforts. You must always ensure that you are aware of what you're looking for. That being said, you cannot expect to protect your system from everything - that's impossible. The only way you can protect your system from absolutely all threats is to unplug it and lock it up in a cupboard to ensure that it's never touched. Let's face it, that isn't the best approach to secure your information. You should only learn to protect your system from common cracker attacks and other well-known vulnerabilities. Some cracker attacks are still unknown, but that doesn't mean that you should give up on testing your system. Try to use different combinations and test the entire system instead of looking at the individual units alone. You will discover more vulnerabilities in your system when you test it as a whole.

It's advisable that you don't take ethical hacking too far. For example, if you don't have too many people working in an office and don't have an internal web server, you needn't worry too much about an attack through the web. However, you should never forget about any malicious employees who will threaten the security of your company.

All in all, your goals as an ethical hacker should be as follows:

- Use a nondestructive approach to hack systems.
- Identify vulnerabilities and use these vulnerabilities to prove that systems need improvements.
- Apply the results and remove any vulnerabilities to improve security.

Ethical Hacking Commandments

There are a few commandments that an ethical hacker must abide by. If a hacker does not abide by those commandments, there will be negative consequences. In the cases that an ethical hacker doesn't follow these commandments, the results are not beneficial.

Working Ethically

In this context, the word "ethical" refers to working with high morals and principles. Regardless of whether you are performing ethical hacking tests on your system or someone hired you to test their system, you must ensure that the steps you take support the goals of the individual or organization. In other words, you cannot have a hidden agenda. You have to ensure that you are honest and never should you misuse any information you find on the system; that is precisely what crackers do.

Respecting Privacy

You must always respect the information that you gather. All the data to which you are granted access during testing should be kept private, right from clear-text passwords to web-application log files. You should never use this information to peek into confidential information or people's private lives. If you sense that there is an issue, you should share that information with the right person. Additionally, you should make a habit of involving other people

in your process to ensure that the owner of the system can trust you.

Not Crashing Systems

Many people crash their systems because they don't have a plan in mind when they begin their testing. These testers have either misunderstood the documentation or have not read it whatsoever. As a result, they don't know how to use different tools to test the security of their systems. If you run too many tests on your system, you can create a DoS condition that causes a system lockup. You should never rush into it or assume that a specific host or network can bear the beating that the vulnerability assessment and network scanner tools dish out.

Many security assessment tools control how tests are performed on systems at the same time. These tools are handy if you need to run a test on systems during business hours. You can create a system lockout condition or lock the account by forcing someone to change their password. These people will not realize that they have agreed to lock their system.

Advantages of Hacking

Hacking is a useful process when you:

- Perform a penetration test to identify any vulnerabilities in the network and computer security
- Recover any lost information, mainly in the case of a lost password
- Identify protection or preventive measures that can be implemented to prevent any breaches in security
- Prevent any unauthorized access from malicious hackers

Disadvantages of Hacking

If hacking is done with negative intention, it can lead to the following issues:

- Privacy violations
- Unauthorized access to private information on a system

- Denial-of-service attacks
- Massive security breaches
- Malicious attacks on the system, leading to loss of important information
- Hampering the operations of the system

Chapter 2

Types of Hackers

A hacker can be placed into one of the following categories: black hat, grey hat or white hat. Each hacker is classified based on their intent. These terms are borrowed from the Old West when a good cowboy would wear a white hat while a bad cowboy would don a black hat.

White Hat Hackers

A white hat hacker, who is also called an ethical hacker, does not want to harm the system. His motive is to identify the weakness in any network system or computer through different vulnerability assessments and penetration testing. Ethical hacking is legal, and, in fact, many companies hire ethical hackers to find vulnerabilities.

Black Hat Hackers

A black hat hacker, who is also known as a cracker, is someone who wants to hack a network or a system to gain unauthorized access. This type of hacker wishes to harm the system or steal some sensitive information. Black hat hacking is illegal since the person who is hacking the system does it with bad intentions. This includes violating privacy, blocking any communication on the network, stealing corporate data, damaging systems, etc.

Grey Hat Hackers

A grey hat hacker is a blend of both a white hat and a black hat hacker. These hackers do not have any malicious intent but hack a network or a system merely for fun. They want to exploit the vulnerabilities in the system without actually taking permission from the owner. Usually, their goal is to inform the owner of any weaknesses and gain appreciation and/or a sum of money from them.

Miscellaneous Hackers

Apart from the list of hackers detailed above, there are a few other categories of hackers that should be mentioned. These include script kiddies, intermediate hackers, elite hackers, hacktivists, cyberterrorists, and hackers involved in organized crime.

Script Kiddies

These hackers are computer novices who use the different tools and documentation available on the Internet to perform a hack. They do not know what happens behind the scenes and only comprehend enough to cause minimal harm. They are often sloppy, so they leave digital fingerprints everywhere. These are the hackers you hear about in the news. They need very minimal skills to attack a system since they use what is already made available to them.

Intermediate Hackers

These hackers know just enough to cause some serious issues. They have knowledge about networks and computers and use this knowledge to carry out well-known exploits. Some intermediate hackers want to be experts at the process; if they put in some effort, they can certainly become elite hackers.

Elite Hackers

Elite hackers are experts. They're the people who develop several hacking tools and write scripts and programs. Script kiddies use these very tools and programs to perform their own attacks. Elite hackers write codes to develop malware like worms and viruses. They know how to break into a system and cover their tracks or pretend that someone else was responsible for the attack.

Elite hackers are secretive and only share information if they believe that their subordinates are worthy. For some lower-level hackers to be evaluated as worthy, they should possess some special information that an elite hacker can use to perform an attack on a high-profile system. Elite hackers are the worst type of hackers. However, there are not too many of them in the world when compared to the number of script kiddies.

Hacktivists

These hackers disseminate social or political messages through their attacks. A hacktivist always finds a way to raise awareness about a given issue. Some

examples of hacktivism are the many websites that had the “Free Kevin” messages. These hacktivists wanted the government to release hacker Kevin Mitnick from prison. Some other cases include the protests against the U.S. Navy Spy Plane that collided with a Chinese fighter jet in 2001, attacks against the U.S. White House website for years, hacker attacks between Pakistan and India and messages supporting the legalization of marijuana.

Cyberterrorists

Cyberterrorists attack government computers or other public utility infrastructures like air-traffic control towers and power grids. They steal classified government information or crash some critical systems. Countries have started to take cyberterrorist threats seriously, ensuring that power companies and other similar industries always have information-security controls in place. These controls will protect systems from such attacks.

Organized Crime

Some groups of hackers can be hired to perform an organized crime. In 2003, the Korean police busted one of the largest hacking rings on the Internet. This ring had close to 4,400 members. In addition to that group, the Philippine police busted a multimillion-dollar hacking ring that sold cheap phone calls made through the lines that the ring had hacked into. These types of hackers are always hired for a large amount of money.

Chapter 3

Ethical Hacking Terminologies

This chapter briefly details some of the common and important terms that are used in the field of hacking.

Adware

Hackers use this software to display advertisements on a system by force.

Attack

Hackers perform this action to access a system and extract some sensitive data from that system.

Back Door

A back door, which is also referred to as a trap door, is an entry port into software or a computer. This port does not require any login information or a password, and as a result, it can bypass all security measures.

Bot

A bot is a type of program that is used to automate any action, thereby increasing the number of times it can be performed. This means that the bot will perform the function for a longer time when compared to a human operator. For instance, hackers use bots to call a script that can be used to create an object or send an FTP< Telnet or HTTP file at a higher rate.

Botnet

Botnets, which are also called zombie armies, are a group of computers that can be controlled without the knowledge of the owner. These are used to perform denial-of-service attacks or send spam.

Brute Force Attack

A brute force attack is possibly the simplest attack that a hacker can perform to gain access to a system or application. This attack is an automated attack, and this means that it will try different usernames and passwords repeatedly until it can access the system or application.

Buffer Overflow

The buffer overflow is a flaw that can be observed when a lot of data is written onto a single block of memory. This means that the memory can no longer hold onto that data.

Clone Phishing

Clone phishing is a type of legitimate and existing email that has a false link. This link will trick a recipient into providing some personal information that the hacker can use to disarm the system or network.

Cracker

A cracker is a type of hacker that modifies any software to access some features of a system, such as copy protection features.

DoS or Denial-of-Service Attack

A denial-of-service, or DoS, attack is used by a hacker to ensure that a network resource or server is not available to the user. This is done by suspending the services of that server or resource.

DDoS

DDos stands for distributed denial-of-service attack.

Exploit Kit

An exploit kit is a system that a hacker designs to run on some web servers. This system is used to identify any vulnerabilities in a client machine that is communicating with the web server. It will then exploit those vulnerabilities and afterwards, execute some malicious code in the system.

Exploit

An exploit is a part of code or a chunk of data or software that will take advantage of a vulnerability or a bug in the system and network which, in turn, compromises the security of that system or network.

Firewall

A firewall is a type of filter that is placed on a network. This filter helps to keep unwanted intruders away from the system or network. In addition, it will ensure that the communication between the users and systems inside the firewall are safe.

Keystroke Logging

Keystroke logging is a process during which a hacker tracks how the keys are pressed on the keypad. This process will help the hacker develop a blueprint of the human interface. It is often used by both black and grey hat hackers to record some passwords. A keylogger is most commonly delivered onto a system using a phishing email or a Trojan horse.

Logic Bomb

A logic bomb is a type of virus that is added to a system that will trigger a malicious attack if some conditions are met. A common example of a logic bomb virus is a time bomb.

Malware

Malware is a term that describes a variety of intrusive and hostile software, including Trojan horses, spyware, scareware, adware, virus, ransomware, worms and any other malicious programs.

Master Program

Master programs are those programs that black hat hackers use to transmit commands into zombie drones (explained later in the chapter). These drones carry spam attacks or denial-of-service attacks.

Phishing

Phishing is a fraud method where the hacker sends an email out to the target. The hacker will use this email to gather some personal or financial information from the user.

Phreaker

A phreaker is a normal computer hacker. These hackers often break into telephone networks and either tap the phone lines or make long-distance phone calls.

Rootkit

Rootkit is a software that is often malicious. A hacker designs this software to hide some processes or programs from any normal detection method. This will ensure that the rootkit is stored on a system and has privileged access to the system.

Shrink Wrap Code

A shrink wrap code attack is a way to exploit the holes in a poorly configured or unpatched software.

Social Engineering

A hacker uses social engineering to deceive another person. The hacker uses this technique to acquire some personal information about the user, like credit card details or passwords.

Spam

Spam is an unsolicited email. This is also called junk email and is often sent to a large group of people without their consent.

Spoofing

Spoofing is a technique that a hacker uses to gain access to a system or network. The hacker will send a message to the computer using an IP address, and this address will indicate to the system that the message is being sent from a trusted host.

Spyware

Spyware is a software that's used to gather information about an organization or person without their knowledge. This software can be utilized to send sensitive information to any entity without the consent of the customer. It can also be used to assert control over a system.

SQL Injection

SQL injection is an injection technique code that is written in SQL. This tool is used to attack any data-driven application. It includes some malicious SQL statements that are entered into a field in the data. An example of an SQL injection would be dumping all data into the attacker's folders.

Threat

Threats are possible dangers to a system or network. These can be used by hackers to exploit a vulnerability and compromise the security of a network or system.

Trojan

A Trojan horse, or Trojan, is a program that is designed to look like a normal program. Differentiating between a Trojan and a regular program is difficult. This tool can be used to alter information, destroy files and steal sensitive information like passwords.

Virus

A virus is a piece of code or a full program that is malicious. It copies itself in the system and has a detrimental effect on it as a result. A virus can both destroy data and corrupt the system.

Vulnerability

A vulnerability is a weakness in the system or network that allows a hacker to compromise the security of that system or network.

Worms

Worms are like every other virus in the sense that it can replicate itself in the

system. It only resides in the active memory but does not make any changes to the files and will only duplicate itself.

Cross-Site Scripting

Cross-site scripting, or XSS, is a security vulnerability that is often found in a web application. This vulnerability gives the hacker the ability to inject some script into a web page that is viewed by users.

Zombie Drone

A zombie drone is used by hackers as a soldier to perform a malicious activity. This drone is a hijacked computer that is used by some hackers to distribute unwanted spam emails.

Chapter 4

Ethical Hacking Tools

Now that you know what ethical hacking is, let's look at some of the different tools that are available for you to use to prevent any unauthorized access to a network system or computer.

Nmap

Nmap, or Network Mapper, is a tool that is used for security auditing and network discovery. It is an open source tool that was designed to scan a large network. It also works well with single hosts. A network administrator is used for different tasks, including managing service upgrade schedules and network inventory and monitoring service or host uptime.

Nmap can determine the following using raw IP packets:

- The different hosts available on the network
- The operating systems that the hosts run on
- The different services offered by those hosts
- The different firewalls that the hosts use and any other characteristics

This tool can run on most operating systems, including Linux, Windows and Mac OS X.

Metasploit

Metasploit, another powerful exploitation tool, is a Rapid7 product. Many of the resources used can be found on the source website www.metasploit.com. The tool has a commercial and free version and can be used with Web UI or command prompt.

You can perform the following operations using Metasploit:

- Penetration tests on small networks
- Check the vulnerability in some systems
- Discover any import or network scan data
- Run individual tests on a host or look at the different modules that one can exploit

Burp Suite

Burp Suite is a tool that's used by both malicious and ethical hackers to perform a security test of any web application. This suite has different tools that work together to support the process of testing, right from the mapping to the analysis of the application's surface. It's often used to exploit or locate any vulnerabilities in the application. This suite is simple to use and gives an administrator full control to combine different techniques to improve testing. Burp can be configured easily, and it has different features that can help an experienced tester with their work.

Angry IP Scanner

Angry IP scanner is a cross-platform and lightweight port and IP address scanner. This tool can scan an IP address in any range and can be used or copied anywhere. It utilizes a multithreading approach to increase the speed of scanning. In this approach, a separate scanning thread is employed for every address. Angry IP scanner checks if an IP address is active by pinging the address, and it will then determine the MAC address and scan ports and resolve the hostname. The data that is gathered using this tool can be saved to an XML, TXT, IP-Port List or CSV file. You can gather information about any IP using this tool.

Cain and Abel

Cain and Abel is a tool used in Microsoft Operating Systems for password recovery. This tool helps to retrieve passwords using one of the following methods:

- Recording a VoIP conversation
- Sniffing the network
- Decoding a scrambled password
- Cracking an encrypted password using Brute-Force, Cryptanalysis and Dictionary
- Revealing a password box
- Recovering wireless network keys
- Uncovering a cached password
- Analyzing routing protocols

This is a tool that most professional penetration testers and security consultants use for ethical hacking.

Ettercap

Ettercap, or Ethernet capture, is a network security tool that's used for a man-in-the-middle attack. This tool can sniff live connections, filter any content on the fly and perform other interesting activities. Ettercap has numerous features that can be used for host and network analysis and supports the dissection of protocols (both active and passive). It runs on many operating systems, including Mac OS X, Linux and Windows.

EtherPeek

EtherPeek is a tool that helps to simplify network analysis that is performed on a heterogeneous network environment. This is a very small tool that can be installed on any system in a few minutes. One can use this tool to sniff the traffic packets on any network and supports different protocols, including IP, AppleTalk, UDP, NBT packets, IP Address Resolution Protocol (ARP), NetBEUI, TCP and NetWare.

SuperScan

SuperScan is a powerful tool that can be used to resolve hostnames and scan

any TCP ports. It has a user-friendly interface that can be used to perform the following functions:

- Port or ping scan using a different IP range
- Scan different ports in the network using a built-in or random range
- Decipher the responses from different hosts connected to the network
- Modify the port description and list using a built-in editor
- Merge different lists to build a new one
- Connect different open ports
- Assign a helper application to a port

QualysGuard

QualysGuard is a suite of tools that can be used to lower the cost of compliance and simplify any security operations. This tool can automate the full area of compliance, auditing and protection for web applications and IT systems. QualysGuard can deliver some critical security intelligence and includes a variety of tools that can be used to detect, monitor and protect the network.

WebInspect

WebInspect is a tool used to assess an application's security. This helps to identify any unknown and known vulnerabilities that exist in the application layer for any tool. It can also be used to check if a server has been configured correctly and helps to test the vulnerability of a system using attacks like cross-site scripting, parameter injection, directory traversal and others.

LC4

LC4 (formerly called L0phtCrack) is a password recovery and auditing application. This tool is used to test the strength of passwords and to sometimes recover a password on Microsoft Windows by using hybrid, brute-

force and dictionary attacks. LC4 is used to retrieve lost Windows passwords, which will help to streamline the process of migration. It also assists in retrieving a lost password for an account.

LANguard Network Security Scanner

A LANguard network security scanner scans a network to identify the devices connected to it. It also provides some information about every node in the network. Using the LANguard network scanner, one can obtain any information about the operating system that's used by every system connected to the network. This tool is also utilized to detect any registry issues and can provide a report in HTML format. You can obtain information regarding the NetBIOS name table, the MAC address and the user logged into the network using this tool.

Network Stumbler

Network Stumbler is a WiFi monitor and scanner that is used on the Windows Operating System. This tool allows a network professional to detect a wide area network. Most hackers utilize this tool to find a wireless network that is not used for broadcasting. Network Stumbler can help you verify if a network has been configured well, detect any interference between wireless networks and test the signal coverage and strength. Additionally, it can be used on any unauthorized connections.

ToneLOC

ToneLOC, or Tone Locator, is a program that was written in the early 90s for MS-DOS. It was used in war dialing computer programs. Through war dialing, one can scan phone numbers using a modem and dial every number that has the same area code. Malicious hackers use this tool to breach security by identifying modems that can be used to enter a network or computer system or guess a user's account. Ethical hackers can use it to detect any unauthorized device on the computer's network.

Chapter 5

Ethical Hacking Skills

This chapter covers the ten most important skills every hacker needs to possess and consistently improve on to become a professional in the field.

Basic Computer Skills

You are probably laughing at this skill; however, it is extremely important for a hacker to understand the basic functions of a computer. You'll need to learn how to use command lines in windows and also understand how to edit the registry and set the networking parameters. These may seem like simple skills, but they're actually very difficult to master. If you make an error in the command line, you will mess up the entire hacking process and make the system more vulnerable than it initially was.

This is a skill that professional hackers build on every chance they get. They believe that there is always room for improvement. Amateurs, on the other hand, may believe they have learned everything there is to about computers and rarely build on the knowledge they already have.

Networking Skills

Once you have mastered your computer skills, you'll need to improve your skills with networking. It's important to know how a network functions and how to tweak it to make it better. The skills mentioned in this section are important to know; DNS, NAT, subnetting, DHCP, IPv4, IPv6, and routers and switches are all things you need to know about. You can learn many of the skills addressed in this section online.

As previously mentioned, oftentimes, amateurs are unaware of the different networking skills they will need to build upon. They may learn one or two of the skills mentioned and then fumble while hacking if they come across a different network. Therefore, any hacker who wants to improve should be aware of the various networking skills they need to have.

Linux Skills

Hackers often use Linux as their operating system. In fact, most tools developed for hackers are only designed for the Linux operating system. Linux can help the hacker achieve his end goal, unlike Windows. So, it's always a good idea to learn Linux. Any professional hacker should be adept at using Linux to hack into a system and identify its vulnerabilities.

Wireshark

Wireshark is a packet analyzer that is an open source tool. It's used by hackers to troubleshoot any network issues, analyze software and communications protocols and also to develop certain protocols for the system.

Expert hackers are versed in utilizing this analyzer to create protocols with ease for the system they are hacking into.

Virtualization

Virtualization is the art of making a virtual version of anything, like a server, storage device, operating system or networking resource. This helps the hacker test the attack that is going to take place before making it live. This also helps the hacker check if he or she has made any mistakes and revise the attack.

Professional hackers use this skill to enhance the effect of the hack they are about to perform. This gives them a perspective on the damage they can do to the software while protecting themselves. An amateur hacker usually does not learn how to cover his tracks. A perfect example for this is the boy from Mumbai who released an episode of Game of Thrones from season 7. Had he covered his tracks better, he would have been able to protect himself. This is why it's important to learn all about virtualization.

Security Concepts

It's vital that a hacker learns about different security concepts and understands the changes made to technology. A person who has a strong hold on security will be able to control different barriers set by the security

administrators for the system they are hacking into.

Learning skills like Secure Sockets Layer (SSL), Public Key Infrastructure (PKI), firewalls, Intrusion Detection System (IDS) and other skills are important for hackers to learn. If you're an amateur, it is advised that you take courses like Security +.

Wireless Technology

This is a technology everybody is familiar with – information is sent using invisible waves as the medium. If you are trying to hack into a wireless device, you have to understand the functioning of that device. Therefore, it's vital that you learn the following encryption algorithms: WPA2, WPA WEP, WPS and the four-way handshake. It is also pertinent to understand the protocol connections, authentication and restrictions that surround wireless technology.

Scripting

This is a skill that every hacker must possess, especially the professionals. If a hacker were to use the scripts written by another hacker, he or she would be discredited for that. Security administrators are always vigilant about any hacking attempt and will identify a new tool, which will help them cope with that attack.

A professional hacker needs to build on this skill and ensure that he or she is good at scripting. Amateurs often depend on the scripts written by other hackers. They may or may not understand the script, which would land them in big trouble.

Database

A database helps a user store data in a structured manner on a computer that can be accessed in various ways. If a hacker wishes to hack into a system's database, he or she would need to be adept at different databases and also understand their functioning. Databases often use SQL to retrieve information whenever necessary. Therefore, it's important to learn these skills before you decide to hack into a database.

Professional hackers always need to know their way around a database to ensure that they make no mistakes and avoid getting caught.

Web Applications

Web applications are software through which you can access the Internet via your browser (Chrome, Firefox, etc.). Over the years, web applications have also become a prime target for hackers. It is extremely advisable that you some spend time understanding the functioning of web applications, as well as the databases that back those applications. This will help you make websites of your own either for phishing or for any other use.

The skills mentioned in this chapter are most important for hackers to develop. Professional hackers work to improve these skills right from the beginning and therefore are adept at hacking into any system easily. It’s important for amateurs to build up these skills.