ALL ■ IN ■ ONE

Gray Hat Hacking

The Ethical Hacker's Handbook

Shon Harris, Allen Harper, Chris Eagle,
Jonathan Ness, and Michael Lester

McGraw-Hill/Osborne
New York • Chicago • San Francisco • Lisbon
London • Madrid • Mexico City • Milan • New Delhi
San Juan • Seoul • Singapore • Sydney • Toronto

The McGraw·Hill Companies

McGraw-Hill/Osborne
2100 Powell Street, 10th Floor
Emeryville, California 94608
U.S.A.

To arrange bulk purchase discounts for sales promotions, premiums, or fund-raisers, please contact **McGraw-Hill**/Osborne at the above address. For information on translations or book distributors outside the U.S.A., please see the International Contact Information page immediately following the index of this book.

Gray Hat Hacking: The Ethical Hacker's Handbook

1234567890 CUS CUS 01987654

ISBN 0-07-225709-1

Vice President & Associate Publisher
Scott Rogers

Director of New Program Development
Gareth Hancock

Project Editor
Patty Mon

Acquisitions Coordinator
Jessica Wilson

Technical Editor
Dave Odom

Copy Editor
Lunaea Hougland

Proofreader
Marian Selig

Indexer
Valerie Perry

Composition
Apollo Publishing Services

Illustrator
Sue Albert

Series Design
Peter F. Hancik

Cover Design
Pattie Lee

This book was composed with Corel VENTURA™ Publisher.

Information has been obtained by **McGraw-Hill**/Osborne from sources believed to be reliable. However, because of the possibility of human or mechanical error by our sources, **McGraw-Hill**/Osborne, or others, **McGraw-Hill**/Osborne does not guarantee the accuracy, adequacy, or completeness of any information and is not responsible for any errors or omissions or the results obtained from the use of such information.

CHAPTER

Ethics of Ethical Hacking

Security professionals should understand where ethical hacking fits in information security, proper use of hacking tools, different types of hacking techniques, and the ethics that surround all of these issues. This chapter will cover the following items:

- Role of ethical hacking in today's world
- Vulnerability assessments versus penetration testing
- How hacking tools are used by security professionals
- General steps of hackers and security professionals
- Ethical issues between a white hat and a black hat hacker

This book has not been compiled and written to be used as a tool by individuals who wish to carry out malicious and destructive activities. It is a tool for people who are interested in extending or perfecting their skills to defend against such attacks and damaging acts.

Let's go ahead and get the commonly asked questions out of the way and move on from there.

> *Was this book written to teach today's hackers how to cause damage in more effective ways?*
>
> **Answer:** No. Next question.
>
> *Then why in the world would you try to teach people how to cause destruction and mayhem?*
>
> **Answer:** You cannot properly protect yourself from threats you do not understand. The goal is to identify and prevent destruction and mayhem, not cause it.
>
> *I don't believe you. I think these books are only written for profits and royalties.*
>
> **Answer:** This book was written to actually teach security professionals what the bad guys already know and are doing. More royalties would be nice, so please buy two copies of this book.

Still not convinced? Why do militaries all over the world study their enemies' tactics, tools, strategies, technologies, and so forth? Because the more you know what your enemy is up to, the better idea you have as to what protection mechanisms you need to put into place to defend yourself.

Most countries' militaries carry out scenario-based fighting exercises in many different formats. For example, pilot units will split their team up into the "good guys" and the "bad guys." The bad guys use the tactics, techniques, and methods of fighting as a specific type of enemy—Libya, Russia, United States, Germany, North Korea, and so on. The goal of these exercises is to allow the pilots to understand enemy attack patterns and to identify and be prepared for certain offensive actions, so they can be properly react in the correct defensive manner.

This may seem like a large leap for you, from pilots practicing for wartime and corporations trying to practice proper information security, but it is all about what the team is trying to protect and the risks involved.

Militaries are trying to protect their nation and its assets. Several governments around the world have come to understand that the same assets they have spent millions and billions of dollars to protect physically are now under different types of threats. The tanks, planes, and weaponry still have to be protected from being blown up, but they are all now run by and are dependent upon software. This software can be hacked into, compromised, or corrupted. Coordinates of where bombs are to be dropped can be changed. Individual military bases still need to be protected by surveillance and military police, which is physical security. Surveillance uses satellites and airplanes to watch for suspicious activities taking place from afar, and security police monitor the entry points in and out of the base. These types of controls are limited in monitoring *all* of the entry points into a military base. Because the base is so dependent upon technology and software—as every organization is today—and there are now so many communication channels present (Internet, extranets, wireless, leased lines, shared WAN lines, and so on), there has to be a different type of "security police" that covers and monitors all of these entry points in and out of the base.

So your corporation does not hold top security information about the tactical military troop movement through Afghanistan, you don't have the speculative coordinates of the location of bin Laden, and you are not protecting the launch codes of nuclear bombs—does that mean you do not need to have the same concerns and countermeasures? Nope. The military needs to protect its assets and you need to protect yours.

The example of protecting military bases may seem extreme, but let's look at many of the extreme things that companies and individuals have had to experience because of poorly practiced information security.

Table 1-1, from *USA Today*, shows the estimated amount it cost corporations and organizations around the world to survive and "clean up" during the aftermath of some

Table 1-1 Malware Damage Estimates (Source: *USA Today*)

Year	Virus/Worm	Estimated Damage
1999	Melissa virus	$80 million
2000	Love Bug virus	$10 billion
2001	Code Red I and II worms	$2.6 billion
2001	Nimda virus	$590 million to $2 billion
2002	Klez worm	$9 billion
2003	Slammer worm	$1 billion

Table 1-2 Downtime Losses (Source: Alinean)

Business Application	Estimated Outage Cost per Minute
Supply chain management	$11,000
E-commerce	$10,000
Customer service	$3,700
ATM/POS/EFT	$3,500
Financial management	$1,500
Human capital management	$1,000
Messaging	$1,000
Infrastructure	$700

of the worst malware incidents to date. An interesting thing about malware is that many people seem to put it in a category different from hacking and intrusions. The fact is that malware has evolved to become one of the most sophisticated and automated forms of hacking. The attacker only has to put in some upfront effort developing the software, and then it is free to do damage over and over again with no more effort from the attacker. The commands and logic within the malware are the same components that many attackers carry out manually.

The company Alinean has put together the cost estimates, per minute, for different organizations if their operations are interrupted. Even if an attack or compromise is not totally successful for the attacker (he does not obtain the asset he is going for), this in no way means that the company is unharmed. Many times attacks and intrusions cause more of a nuisance and they can negatively affect production and the operations of departments, which always correlate to costing the company money in direct or indirect ways. These costs are shown in Table 1-2.

A conservative estimate from Gartner pegs the average hourly cost of downtime for computer networks at $42,000. A company that suffers from worse than average downtime of 175 hours a year can lose more than $7 million per year. Even when attacks are not newsworthy enough to be reported on TV or talked about in security industry circles, they still negatively affect companies' bottom lines all the time.

A few more examples and trends of the security compromises and patterns that are taking place today:

- Gartner reports that there are about 600 successful website compromises a day.
- In 2003, identity theft and fraud cost Americans close to $437 million. There were 215,000 identity theft reports, up 33 percent from the year before. (Source: Federal Trade Commission)
- The Radicati Group predicts that by the end of 2004, spam will account for 52 percent of all e-mail messages. They estimate that spam will cost corporations approximately $41.6 billion, which is a 103 percent increase from 2003.
- Internet fraud complaints in the U.S. rose from 16,775 to 48,252 between the end of December 2001 and December 2002. Internet auction fraud made up 46

percent of these, and 31 percent were complaints of nondelivery of merchandise. (Source: Internet Fraud Complaint Center)

- VeriSign has reported that 6.2 percent of all e-commerce transactions in 2003 were fraudulent and that the U.S. leads other countries in terms of attempted fraud transactions—47.8 percent of worldwide fund attempts.
- Financial losses due to computer crimes may run as high as $10 billion a year, according to the February 3, 2004 issue of *Fortune* magazine.
- According to the Gartner research firm, by 2005, 60 percent of security breach incident costs incurred by businesses will be financially or politically motivated.
- $10 million is how high the indirect costs associated with a theft can rise for a company over 500 employees in size. The following are some examples of these indirect costs:
  - Downstream liabilities
    - Systems commandeered for DDoS attacks on others
  - Potential civil legalities
    - Servers commandeered for distribution of illegal information—such as music and porn
  - Potential civil, local, state, and federal legalities
- The Securities and Exchange Commission (SEC) fined five firms (Deutsche Bank Securities, Goldman Sachs, Morgan Stanley, Salomon Smith Barney, and U.S. Bancorp Piper Jaffray) $8.25 million ($1.65 million each, not counting legal fees and bad PR) for violating record-keeping requirements in regard to preserving e-mail communications. (See www.sec.gov/news/press/2002-173.htm.)
- On July 25, 2002, NYS AG Spitzer announced a multi-state agreement with Eli Lilly for an incident in 2001 wherein the pharmaceutical manufacturer inadvertently revealed approximately 670 Prozac subscribers' e-mail addresses. The agreement outlined security measures that Eli Lilly must take, along with $160,000 in fines. (See www.oag.state.ny.us/press/2002/jul/jul25c_02.html.)
- Subscriber information, including credit card numbers, were stolen from one of Ziff Davis' magazine promotion sites. The Attorney General's office took notice of the data theft and found ZD's privacy policy and ZD's interpretation of "reasonable security controls" to be inadequate. This resulted in $100,000 in state fines or $500 per credit card lost and a detailed agreement outlining security control requirements. (See www.oag.state.ny.us/press/2002/aug/aug28a_02.html.)

CERT shows in their Cyberterrisom study in May 2002 that the bad guys are getting smarter, more resourceful, and seemingly unstoppable, as shown in Figure 1-1.

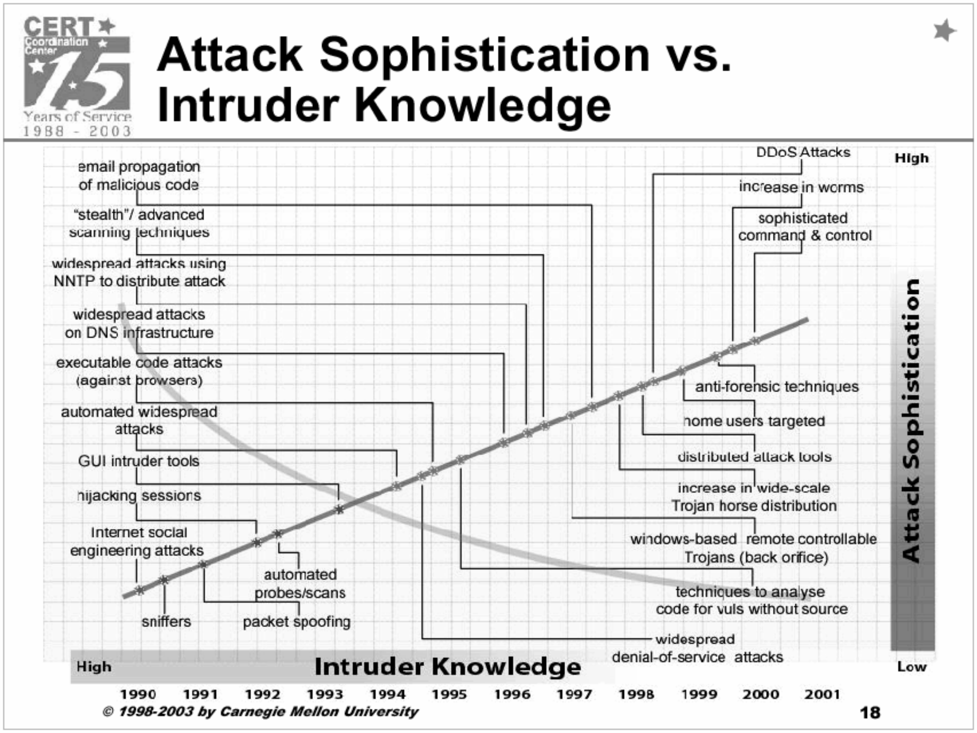

Figure 1-1 The sophistication and knowledge of hackers are increasing.

So what will companies need to do to properly protect themselves from these types of incidents and business risks?

- In 2005, security will become more strategic as companies invest greater resources in developing strategies, defining architectures, and carrying out risk assessments. Organizational priorities will include training staff, educating employees, and developing policy and standards (Source: A Worldwide Study Conducted by *CIO Magazine* and PricewaterhouseCoopers)
- In 2002, businesses spent around 12 percent of their IT budgets on security, according to *InformationWeek*'s 2002 Global Information Security Survey, fielded by PricewaterhouseCoopers. Today it is closer to 20 percent.
- Security and business continuity were top priorities for 29 percent of companies in 2003 as they developed their IT spending plans. (Source: AMR Research)

- By 2007 it is expected that the secure content management (SCM) software market will grow from $236 million in 2002 to $1.1 billion. (Source: International Data Corporation)
- By 2007 the web filtering business is projected to reach $893 million and antivirus software will reach up to $6.4 billion. (Source: International Data Corporation)
- Various web application security products and services had an estimated market value of $140 million in 2002. They are reaching their forecasted $500 million in 2004, and are projected to be a $1.74 billion industry by 2007. (Source: The Yankee Group)
- Hacker insurance is expected to jump from a $100 million market today to $900 million by 2005. (Source: Gartner)
    - American International Group (AIG) recently created stand-alone coverage for viruses and credit card and ID theft.

References

Federal Trade Commission—Consumer Information Security www.ftc.gov/infosecurity/

Federal Trade Commission—Information Privacy and Security www.ftc.gov/privacy/

About the Internet Fraud Complaint Center www.fbi.gov/hq/cid/fc/ifcc/about/about_ifcc.htm

CERT Advisories www.cert.org/advisories/

CSI/FBI 2000 Computer Crime and Security Survey www.pbs.org/wgbh/pages/frontline/shows/hackers/risks/csi-fbi2000.pdf

How Does This Stuff Relate to an Ethical Hacking Book?

Corporations and individuals need to understand *how* these damages are taking place so they can understand how to stop them. Corporations also need to understand the extent of the threat that a vulnerability provides. For example, the company FalseSenseOfSecurity, Inc., may allow their employees to share out directories, files, and their whole hard drives. This is done so that others can quickly and easily access data as needed. The company may understand that this practice could possibly put the files at risk, but they only allow employees to have unclassified files on their computers, so the company is not overly concerned. The real security threat, which is something that should be uncovered by an ethical hacker, is if an attacker can use this file-sharing service as access into a computer itself. Once this computer is compromised, the attacker will most likely plant a backdoor and work on accessing another, more critical system via the compromised system.

The vast amount of functionality that is provided by organizations' networking, database, and desktop software is also the thing that attackers use against them. There is an all too familiar battle of functionality vs. security within each and every organization. This is the reason that in most environments the security officer is not the most well-liked individual in the company. Security officers are in charge of ensuring the overall security of the environment, which usually means reducing or shutting off many functionalities that users love. Telling people that they cannot use music-sharing software, open attachments, use applets or JavaScript via e-mail, or disable the antivirus software that slows down software procedures, and making them attend security awareness training does not usually get you invited to the Friday night get-togethers at the bar. Instead these people are often called "Security Nazi" or "Mr. No" behind their backs. They are responsible for the balance between functionality and security within the company, and it is a hard job.

The ethical hacker's job is to find many of these things that are running on systems and networks, and they need to have the skill set to know how an enemy would use them against the organization. This work is referred to as a penetration test, which is different from a vulnerability assessment.

Vulnerability Assessment

A vulnerability assessment is usually carried out by a network scanner on steroids. Some type of automated scanning product is used (Nessus, Retina, Heat, Internet Security Scanner, and such) to probe the ports and services on a range of IP addresses. Most of these products can also test for the type of operating system and application software running, the versions, patch levels, user accounts, and SNMP Management Information Base (MIB) data. They may carry out a low-level password brute-force attack. These findings are matched up with correlating vulnerabilities in the product's database. The end result is a large pile of paper that provides a list of each system's vulnerabilities and corresponding countermeasures to mitigate the associated risks. Basically, the tool states, "Here is a list of your vulnerabilities and here is a list of things you need to do to fix them."

NOTE SNMP uses a MIB to hold a vast amount of system status information. In most cases, this data is easily accessible to attackers and allows them to map out a network and its resources and possibly reconfigure critical devices.

To the novice, this sounds like an open and shut case and an easy stroll into network utopia where all of the scary entities can be kept out. This false utopia, unfortunately, is created by not understanding the complexity of information security. The problem with just depending upon this large pile of printouts is that it was generated by an automated tool that has a hard time putting its findings into the proper context of the given environment. For example, several of these tools provide an alert of "High" for vulnerabilities that do not have a highly probable threat associated with them. The tools also cannot understand how a small, seemingly insignificant vulnerability can be used in a large orchestrated attack.

Vulnerability assessments are great for identifying the foundational security issues within an environment, but many times it takes an ethical hacker to really test and qualify the level of risk specific vulnerabilities provide.

Penetration Testing

A penetration test is when ethical hackers do their magic. They can test many of the vulnerabilities identified during the vulnerability assessment to quantify the actual threat and risk of the vulnerability, or it can be a stand-alone procedure. In the stand-alone procedure, the ethical hacker would do her best to break into the company's network to prove that it can be done.

When ethical hackers are carrying out a penetration test, their ultimate goal is to break into a system and hop from system to system until they "own" the domain or environment. They own the domain or environment when they have either root privileges on the most critical Unix system or domain administrator account that can access and control all of the resources on the network. They do this to show the customer (company) what an actual attacker can do under the circumstances and current security posture of the network.

Many times, while the ethical hacker is carrying out her procedures to gain total control of the network, she will pick up significant trophies along the way. These trophies can include the CEO's passwords, company trade secret documentation, administrative passwords to all border routers, documents marked "confidential" held on the CFO and CIO laptops, or the combination to the company vault. The reason these trophies are collected along the way is to allow the decision makers to understand the ramifications of these vulnerabilities. A security professional can go on for hours to the CEO, CIO, or COO about services, open ports, misconfigurations, and hacker potential without making a point that this audience understands or cares about. But as soon as you show the CFO his next year's projections, show the CIO all of the blueprints to the next year's product line, or tell the CEO that his password is "IAmWearingPanties," they will all want to learn more about the importance of a firewall and other countermeasures that should be put into place.

CAUTION No security professional should ever try to embarrass a customer or make them feel inadequate for their lack of security. This is why the security professional has been invited into the environment. He is a guest and is there to help solve the problem, not point fingers. Also, in most cases any sensitive data should not be read by the penetration team because of the possibilities of future lawsuits pertaining to the use of confidential information.

The vulnerability test has the goal of providing a listing of all of the vulnerabilities within a network. The penetration test has the goal of showing the company how these vulnerabilities can be used against it by attackers. From here the security professional provides advice on the necessary countermeasures that should be implemented to reduce the threats of these vulnerabilities individually and collectively. In this book, we will cover advanced vulnerability tools and methods as well as sophisticated penetration techniques. Then we'll dig into the programming code to show you how skilled attackers identify vulnerabilities and develop new tools to exploit their findings.

References

The Pros and Cons of Ethical Hacking www.enterpriseitplanet.com/security/features/article.php/3307031

CICA Penetration Testing White Paper www.cica.ca/index.cfm/ci_id/15758/la_id/1.htm

NIST-800-42 http://csrc.nist.gov/publications/

Penetration Testing for Web Applications www.securityfocus.com/infocus/1704

The Controversy of Hacking Books and Classes

When books on hacking first came out, a big controversy arose pertaining to whether this was the right thing to do or not. One side said that such books only increased the attackers' skills and techniques and created new attackers. The other side stated that the attackers already had these skills and these books were written to bring the security professionals and networking individuals up to speed. Who was right? They both were.

The word "hacking" is sexy, exciting, seemingly seedy, and usually brings about thoughts of complex technical activities, sophisticated crimes, and a look into the face of electronic danger itself. Although some computer crimes may take on *some* of these aspects, in reality it is not this grand or romantic. A computer is just a new tool to carry out old crimes.

Attackers are only one component of information security. Unfortunately, when most people think of security their minds go right to packets, firewalls, and hackers. Security is a much larger and more complex beast than these technical items. Real security includes policies and procedures, liabilities and laws, human behavior patterns, corporate security programs and implementation, and yes, the technical aspects—firewalls, intrusion detection systems, proxies, encryption, antivirus software, hacks, cracks, and attacks.

Understanding how different types of hacking tools are used and how certain attacks are carried out is just one piece of the puzzle. But like all pieces of a puzzle, it is very important. For example, if a network administrator implements a packet filtering firewall and sets up the necessary configurations, he may feel the company is now safe and sound. He has configured his access control lists to only allow "established" traffic into the network. This means that an outside source cannot send a SYN packet to initiate communication with an inside system. If the administrator did not realize that there are tools that allow for ACK packets to be generated and sent, he is only seeing part of the picture here. This lack of knowledge and experience allows for a false sense of security, which seems to be pretty common in companies around the world today.

Let's look at another example. A network engineer configures a firewall to review only the first fragment of a packet and not the packet fragments that follow. The engineer knows that this type of "cut through" configuration will increase network performance. But if she is not aware that there are tools that can create fragments with dangerous payloads, she could be allowing in malicious traffic. Once these fragments reach the inside destination system and are reassembled, the packet can be put back together and initiate an attack.

In addition, if a company's employees are not aware of social engineering attacks and how damaging they can be, they may happily give out useful information to attackers. This information is then used to generate even more powerful and dangerous attacks against the company. Knowledge and the implementation of knowledge are the keys for any real security to be accomplished.

So where do we stand on hacking books and hacking classes? Directly on top of a slippery banana peel. There are currently three prongs to the problem of today's hacking classes and books. First, marketing people love to use the word "hacking" instead of more meaningful and responsible labels such as "penetration methodology." This means that too many things fall under the umbrella of hacking. All of these procedures now take on the negative connotation that the word "hacking" has come to be associated with. Second is the educational piece of the difference between hacking and ethical hacking, and the necessity of ethical hacking (penetration testing) in the security industry. The third issue has to do with the irresponsibility of many hacking books and classes. If these items are really being developed to help out the good guys, then they should be developed and structured that way. This means more than just showing how to exploit a vulnerability. These educational components should show the necessary countermeasures required to fight against these types of attacks and how to implement preventive measures to help ensure that these vulnerabilities are not exploited. Many books and courses tout the message of being a resource for the white hat and security professional. If you are writing a book or curriculum for black hats, then just admit it. You will make just as much (or more) money, and you will help eliminate the confusion between the concepts of hacking and ethical hacking.

The Dual Nature of Tools

In most instances, the toolset used by malicious attackers is the same toolset used by security professionals. A lot of people do not seem to understand this. In fact, the books, classes, articles, websites, and seminars on hacking could be legitimately renamed to "security professional toolset education." The problem is that marketing people like to use the word "hacking" because it draws more attention and paying customers.

As covered earlier, ethical hackers go through the same processes and procedures as unethical hackers, so it only makes sense that they use the same basic toolset. It would not be useful to prove that attackers could not get through the security barriers with Tool A if attackers do not use Tool A. The ethical hacker has to know what the bad guys are using, know the new exploits that are out in the underground, and continually keep her skills and knowledgebase up to date. This is because the odds are against the company and against the security professional. The reason is that the security professional has to identify and address all of the vulnerabilities in an environment. The attacker only has to be really good at one or two exploits, or really lucky. A comparison can be made to the U.S. Homeland Security responsibilities. The CIA and FBI are responsible for protecting the nation from the 10 million things terrorists could possibly think up and carry out. The terrorist only has to be successful at *one* of these 10 million things.

NOTE Many ethical hackers engage themselves in the hacker community so they can learn about the new tools and attacks that are about to be used on victims.

How Are These Tools Used for Good Instead of Evil?

How would a company's networking staff ensure that all of the employees are creating complex passwords that meet the company's password policy? They can set operating system configurations to make sure the passwords are of a certain length, contain upper- and lowercase letters, contain numeric values, and keep a password history. But these configurations cannot check for dictionary words or calculate how much protection is being provided from brute-force attacks. So the team can use a hacking tool to carry out dictionary and brute-force attacks on individual passwords to actually test their strength. The other choice is to go to each and every employee and ask what their password is, write down the password, and eyeball it to determine if it is good enough. Not a good alternative.

NOTE A company's security policy should state that this type of password testing activity is allowed by the IT staff and security team. Breaking employees' passwords could be seen as intrusive and wrong if management does not acknowledge and allow for such activities to take place. Make sure you get permission before you undertake this type of activity.

The same network staff needs to make sure that their firewall and router configurations will actually provide the protection level that the company requires. They could read the manuals, make the configuration changes, implement ACLs, and then go and get some coffee. Or they could implement the configurations and then run tests against these settings to see if they are allowing malicious traffic in what they thought was controlled. These tests often require the use of hacking tools. The tools carry out different types of attacks, which allow the team to see how the perimeter devices will react in certain circumstances.

Nothing should be trusted until it is tested. There is an amazing number of cases where a company does everything seemingly correct when it comes to their infrastructure security. They implement policies and procedures, roll out firewalls, IDS, and antivirus, have all of their employees attend security awareness training, and continually patch their systems. It is unfortunate that these companies put forth all the right effort and funds only to end up on CNN as the latest victim who had all of their customers' credit card numbers stolen and posted on the Internet. This can happen because they did not carry out the necessary vulnerability and penetration tests.

Every company should decide whether their internal employees will learn and maintain their skills in vulnerability and penetration testing, or if an outside consulting service will be used, and then ensure that testing is carried out in a continual scheduled manner.

References

Tools www.hackingexposed.com/tools/tools.html

Top 75 Network Security Tools www.insecure.org/tools.html

2003 Most Popular Hacking Tools www.thenetworkadministrator.com/2003MostPopularHackingTools.htm

Recognizing Trouble When It Happens

Network administrators, engineers, and security professionals need to be able to recognize when an attack is underway or when one is about to take place. It may seem as though recognizing an attack as it is happening should be easily accomplished. This is only true for the very "noisy" attacks or overwhelming attacks as in denial-of-service (DoS) attacks. Many attackers fly under the radar and go unnoticed by security devices and staff members. It is important to know *how* different types of attacks take place so they can be properly recognized and stopped.

Security issues and compromises are not going to go away any time soon. People who work in positions within corporations that touch security in any way should not try to ignore it or treat security as though it is an island unto itself. The bad guys know that to hurt an enemy is to take out what that victim depends upon most. Today the world is only becoming more dependent upon technology, not less. Even though application development and network and system configuration and maintenance are complex, security is only going to become more entwined with them. When a network staff has a certain level of understanding of security issues and how different compromises take place, they can act more effectively and efficiently when the "all hands on deck" alarm is sounded. In ten years there will not be such a dividing line between security professionals and network engineers. Network engineers will be required to carry out tasks of a security professional, and security professionals will not make such large paychecks.

It is also important to know when an attack may be around the corner. If a network staff is educated on attacker techniques and they see a ping sweep followed a day later by a port scan, they will know that most likely in three days their systems will be attacked. There are many activities that lead up to different attacks, so understanding these items will help the company protect itself. The argument can be made that we have more automated security products that identify these types of activities so that we don't have to. But it is very dangerous to just depend upon software that does not have the ability to put the activities in the necessary context and make a decision. Computers can outperform any human on calculations and performing repetitive tasks, but we still have the ability to make some necessary judgment calls because we understand the grays in life and do not just see things in 1s and 0s.

As many network engineers understand, IDS may be a wonderful and engaging technology, but it is still immature. A network engineer who learns how to quickly identify false alarms (non-attacks) and properly calibrate the IDS product will provide a lot more protection than the engineer who just chalks the product up to a waste of time and money and disables it.

So it is important to see how hacking tools are really just software tools that carry out some specific type of procedure to achieve a desired result. The tools can be used for good (defensive) purposes or for bad (offensive) purposes. The good and the bad guys use the exact same toolset, it is just the intent that is practiced when operating these utilities. It is imperative for the security professional to understand how to use these tools and how attacks are carried out if he is going to be of any use to his customer and to the industry.

Emulating the Attack

Once network administrators, engineers, and security professionals understand how attackers work, then they can be able to emulate their activities if they plan on carrying out a useful penetration test. But why would anyone want to emulate an attack? Because this is the only way to truly test an environment's security level—how it will react when a real attack is being carried out on it. The common steps for attackers are shown in Table 1-3.

This book is laid out to walk you through these different steps so that you can understand how many types of attacks take place. It can help you develop methodologies of how to emulate similar activities to test your company's security level.

There are already many elementary ethical hacking books available in every bookstore. The demand for these books and hacking courses over the years has shown the interest and the need in the market. It is also obvious that although some people are just entering this sector, many individuals are ready to move on to the more advanced topics of ethical hacking. The goal of this book is to quickly go through some of the basic ethical

Steps in Attack	Explanation	Examples
Reconnaissance	Intelligence work of obtaining information, either passively or actively	**Passively** Sniffing traffic, eavesdropping **Actively** Obtaining data from ARIN and Whois databases, examining website HTML code, social engineering
Scanning	Identifying systems that are running and the services that are active on them	Ping sweeps and port scans
Gaining access	Exploiting identified vulnerabilities to gain unauthorized access	Exploiting a buffer overflow or brute-forcing a password and logging onto a system
Maintaining access	Uploading malicious software to ensure re-entry is possible	Installing a backdoor on a system
Covering tracks	Carrying out activities to hide one's malicious activities	Deleting or modifying data in system and application logs

Table 1-3 Attack Steps

hacking concepts and spend more time with the concepts that are not readily available to you, but are unbelievably important.

Just in case you choose to use the information in this book for unintended purposes (malicious activity), in the next chapters we will also walk through several federal laws that have been put into place to scare you away from this. A wide range of computer crimes are taken seriously by today's court system, and attackers are receiving hefty fines and jail sentences for their activities. Don't let it be you. There is just as much fun and intellectual stimulation to be had working as a white hat, with no threat of jail time!

Where Do Attackers Have Most of Their Fun?

Hacking into a system and environment is almost always carried out by exploiting vulnerabilities in software. Only recently has the light started to shine on the root of the problem of successful attacks and exploits, which is flaws within software code. Every attack method described in this book can be carried out because of errors in the software.

It is not fair to put all of the blame on the programmers, because they have done exactly what their employers and market have asked them to: quickly build applications with tremendous functionality. Only over the last few years has the market started screaming for functionality and security, and the vendors and programmers are scrambling to meet these new requirements and still stay profitable.

Security Does Not Like Complexity

Software in general is very complicated, and the more functionality that we try to shove into applications and operating systems, the more complex software will become. The more complex software gets, the harder it is to properly predict how it will react in all possible scenarios, and it becomes much harder to secure.

Today's operating systems and applications are increasing in lines of code (LOC). Windows XP has approximately 40 million LOC, Netscape 17 million LOC, and Windows 2000 around 29 million LOC. Unix and Linux operating systems have much less, usually around 2 million LOC. A common estimate used in the industry is that there are between 5–50 bugs per 1,000 lines of code. So a middle of the road estimate would be that Windows XP has approximately 1,200,000 bugs. (Not a statement of fact. Just a guesstimation.)

It is difficult enough to try to logically understand and secure 17–40 million LOC, but the complexity does not stop there. The programming industry has evolved from traditional programming languages to object-oriented languages, which allow for a modular approach to developing software. There are a lot of benefits to this approach: reusable components, faster to market times, decrease in programming time, and easier ways to troubleshoot and update individual modules within the software. But applications and operating systems use each other's components, users download different types of mobile code to extend functionality, DLLs are installed and shared, and instead of application-to-operating system communication, today many applications communicate directly with each other. This does not allow for the operating system to control this type of information flow and provide protection against possible compromises.

If we peek under the covers even further we see that thousands of protocols are integrated into the different operating system protocol stacks, which allows for distributed computing. The operating systems and applications must rely on these protocols for transmission to another system or application, even if the protocols contain their own inherent security flaws. Device drivers are developed by different vendors and installed into the operating system. Many times these drivers are not well developed and can negatively affect the stability of an operating system. And to get even closer to the hardware level, injection of malicious code into firmware is an up and coming attack avenue.

So is it all doom and gloom? Yep, for now. Until we understand that a majority of the successful attacks are carried out because software vendors do not integrate security into the design and specification phases, that our programmers have not been properly taught how to code securely, vendors are not being held liable for faulty code, and consumers are not willing to pay more for properly developed and tested code, our staggering hacking and company compromise statistics will only increase.

Will it get worse before it gets better? Probably. Every industry in the world is becoming more reliant on software and technology. Software vendors have to carry out the continual one-upmanship to ensure their survivability in the market. Although security is becoming more of an issue, functionality of software has always been the main driving component of products and it always will be.

Will vendors integrate better security, ensure their programmers are properly trained in secure coding practices, and put each product through more and more testing cycles? Not until they have to. Once the market truly demands that this level of protection and security is provided by software products and customers are willing to pay more for security, then the vendors will step up to the plate. Currently most vendors are only integrating protection mechanisms because of the backlash and demand from their customer bases. Unfortunately, just as September 11th awakened the United States to its vulnerabilities, something large may have to take place in the compromise of software before the industry decides to properly address this issue.

So we are back to the original question: what does this have to do with ethical hacking? A novice ethical hacker will use tools developed by others who have uncovered specific vulnerabilities and methods to exploit them. A more advanced ethical hacker will not just depend upon other people's tools, but will have the skill set and understanding to look at the code itself. The more advanced ethical hacker will be able to identify possible vulnerabilities and programming code errors, and develop ways to rid the software of these types of flaws.

References

SANS Top 20 Vulnerabilities—The Experts Consensus www.sans.org/top20/

Latest Computer Security News www.securitystats.com

Internet Storm Center www.incidents.org

Hackers, Security, Privacy www.deaddrop.org/sites.html

Summary

- Today we are too dependent upon perimeter security devices: routers, firewalls, IDS, and antivirus software.
- By using this "hard outside and soft, chewy inside" enterprise approach, we are not addressing the real problems of network and system security.
- If the software did not contain 5–50 exploitable bugs within every 1,000 lines of code, we would not have to build the fortresses we are constructing today. Use this book as a guide to bring you deeper and deeper under the covers to allow you to truly understand where the security vulnerabilities reside and what should be done about them.

Questions

1. Which of the following is not a reason why governments' militaries are developing and integrating cyberwarfare into their tactical and strategic plans?

   A. Military bases have many more entry points than the traditional physical avenues.

   B. Tanks, aircrafts, weapons, and communication depend upon software and technology.

   C. The last goal in war is to disrupt the enemy's communication.

   D. A tremendous amount of intelligence work is done through monitoring electrical signals.

2. According to Gartner, in year 2005, ____ percent of security compromises will be _______ or __________ motivated.

   A. 60 percent—financially—politically

   B. 40 percent—revenge—financially

   C. 70 percent—financially—educationally

   D. 20 percent—politically—financially

3. Which of the following is generally the most expensive component for organizations when some type of attack takes place?

   A. Legal issues

   B. PR problems

   C. Operational issues

   D. Countermeasure expenses

4. Which of the following best describes the difference between hacking and ethical hacking?

   A. Ethical hacking is done for offensive reasons, where hacking is done for defensive reasons.

B. Ethical hacking is done for defensive reasons, where hacking is done for offensive reasons.

C. Hacking and ethical hacking are the same thing, because the same toolset is used.

D. Hacking and ethical hacking differ only by the tools and skill sets that are used.

5. Which of the following answers is not a reason why company employees should understand how attacks take place?

A. This insight can be used in offensive techniques when needed.

B. This insight can be used to identify when an attack is around the corner.

C. This understanding can better prepare staff members to detect and react to attacks.

D. This understanding can relate to better configurations of countermeasures.

6. There are several reasons why so many different attacks are successful today. Which of the following reasons is not an example of this?

A. The LOC of software is increasing.

B. The use of mobile code is decreasing.

C. The functionality of software is increasing.

D. The complexity of software and its integration methods with other software is increasing.

7. Which of the following is a true statement?

A. More and more software vendors are implementing security in effort to protect the nation's infrastructure.

B. Customers are willing to pay more for security if needed and vendors are willing to increase the delay in product delivery for the purposes of security.

C. Vendors will not increase security in software until the market truly demands it.

D. It is not up to the customers or the vendors to worry about programming flaws.

8. The best reason for studying and understanding ethical hacking can be described how?

A. To advance the level and sophistication of the types of attacks that can be carried out

B. To advance the hacker's skill set so that they can identify organizations' vulnerabilities

C. To advance and increase the degree of damage that can result from certain types of attacks

D. To advance the knowledge and skill set to better protect from malicious activity

Answers

1. **C.** The first goal in war is to disrupt the enemy's communication capabilities. Today, most nations rely heavily on software and technology for their communication procedures. So understanding the vulnerabilities of this technology can be used in a defensive manner (protect one's own communication) and offensive manner (know how to interrupt or destroy another's communication). All other answers are reasons why militaries are building information warfare units.
2. **A.** According to the Gartner research firm, in 2005, 60 percent of security breach incident costs incurred by businesses will be financially or politically motivated. This is a very important issue. Today, we have basically two types of attackers: joy riders who do not go after a specific target with a specific goal, and organized hackers who zero in on an explicit victim for a precise reason. As the legal system advances in tracking down individuals and the penalties increase for this type of activity, the script kiddies and joy riders will start dropping off the map. The organized criminals will only increase their skill set and not be as deterred by increased penalties. More and more people are realizing that computers are just tools to carry out traditional crimes, so more and more criminals will move to these tools because of the amount of anonymity they can provide.
3. **C.** Although many companies that endure large computer attacks can be financially affected by the negative affects on their reputation and can incur legal fines, this is not usually the biggest hit to the pocketbook. Companies today lose most in downtime, loss of productivity and revenue streams, and operational efforts of trying to restore the company back to a working environment.
4. **B.** "Hacking tools" are really just software tools that carry out some specific type of procedure to achieve a desired result. The tools can be used for good (defensive) purposes or for bad offensive) purposes. The good and bad guys use the exact same toolset, what differs is the intent when operating these utilities. It is imperative for the security professional to understand how to use these tools and how attacks are carried out if he is going to be of any use to his customer and to the industry.
5. **A.** Employees should never carry out attacks in an offensive manner against anyone. Employees should use the knowledge, tools, and skill set to test the company's protection level in order to help improve upon it. This insight will also improve upon the proper configuration of the necessary security mechanisms. A company can be held civilly or criminally liable if its employees carry out attacks on individuals or other companies.
6. **B.** The complexity of software is increasing because the demand for functionality and the lines of code are increasing. Applications and operating systems use each other's components, users download different types of mobile code to extend functionality, DLLs are installed and shared, and instead of application-to-operating system communication, today many applications communicate directly with each other. The use of mobile code is increasing, not decreasing.

7. **C.** Until we understand that a majority of the successful attacks are carried out because software vendors do not integrate security into the design and specification phases, that our programmers have not been properly taught how to code securely, vendors are not being held liable for faulty code, and consumers are not willing to pay more for properly developed and tested code, our staggering hacking and company compromise statistics will only increase.
8. **D.** As most countries' militaries carry out scenario-based fighting exercises in many different formats to understand the enemy's tactics, so should security professionals. The goal of these exercises is to allow the security professionals to understand enemy attack patterns, and to identify and be prepared for certain offensive actions, so they can be properly prepared and react in the correct defensive manner. Answers A, B, and C are things we are trying to protect *against*.