Ethical Hacking

Ajinkya A. Farsole
Ethical Hacking Procedure
15, Sujay Nagar,
Sewagram Road, Wardha

Amruta G. Kashikar
Certified Ethical Hacking
Gopuri Chowk,
Nagpur Road, Wardha

Apurva Zunzunwala
Ethical Hacking : Future
State Bank Colony,
Nagpur Road, Wardha

Abstract

One of the fastest growing areas in network security, and certainly an area that generates much discussion is that of ethical hacking. In today's context where the communication techniques have brought the world together; have also brought into being anxiety for the system owners all over the globe. The main reason behind this insecurity is Hacking- more specifically cracking the computer systems. Thus the need of protecting the systems from the nuisance of hacking generated by the hackers is to promote the persons who will punch back the illegal attacks on our computer systems, The Ethical Hackers. The main purpose of this study is to reveal the brief idea of the ethical hacking and its affairs with the corporate security. This paper encloses the epigrammatic disclosure about the Hacking and as well the detailed role of the ethical hacking as the countermeasure to cracking in accordance with the corporate security as well as the individual refuge. This paper tries to develop the centralized idea of the ethical hacking and all its aspects as a whole.

1. INTRODUCTION

The explosive growth of the Internet has brought many good things: electronic commerce, easy access to vast stores of reference material, collaborative computing, e-mail, and new avenues for advertising and information distribution, to name a few. As with most technological advances, there is also a dark side: criminal hackers. Governments, companies, and private citizens around the world are anxious to be a part of this revolution, but they are afraid that some hacker will break into their Web server and replace their logo with pornography, read their e-mail, steal their credit card number from an on-line shopping site, or implant software that will secretly transmit their organization's secrets to the open Internet. With these concerns and others, the ethical hacker can help. This paper describes ethical hackers: their skills, their attitudes, and how they go about helping their customers find and plug up security holes. With the growth of the Internet, computer security has become a major concern for businesses and governments. They want to be able to take advantage of the Internet for electronic commerce, advertising, information distribution and access, and other pursuits, but they are worried about the possibility of being "hacked." At the same time, the potential customers of these services are worried about maintaining control of personal information that varies from credit card numbers to social security numbers and home addresses.In their search for a way to approach the problem, organizations came to realize that one of the best ways to evaluate the intruder threat to their interests would be to have independent computer security professionals attempt to break into their computer systems. This scheme is similar to having independent auditors come into an organization to verify its bookkeeping records. In the case of computer security, these "tiger teams" or "ethical hackers" would employ the same tools and techniques as the intruders, but they would neither damage the target systems nor steal information. Instead, they would evaluate the target systems' security and report back to the owners with the vulnerabilities they found and instructions for how to remedy them.

2. HISTORY OF HACKING

2.1 PREHISTORY

1960s: The Dawn of Hacking
Original meaning of the word "hack" started at MIT; meant elegant, witty or inspired way of doing almost anything; hacks were programming shortcuts

2.2 ELDER DAYS (1970-1979)

1970s: Phone Phreaks and Cap'n Crunch: One phreak, John Draper (aka "Cap'n Crunch"), discovers a toy whistle inside Cap'n Crunch cereal gives 2600-hertz signal, and can access AT&T's long-distance switching system.
Draper builds a "blue box" used with whistle allows Phreaks to make free calls.
Steve Wozniak and Steve Jobs , future founders of Apple Computer, make and sell blue boxes.

2.3 THE GOLDEN AGE (1980-1991)

1980: Hacker Message Boards and Groups
Hacking groups form; such as Legion of Doom (US), Chaos Computer Club (Germany).
1983: Kids' Games
Movie "War Games" introduces public to hacking.

2.4 THE GREAT HACKER WAR

Legion of Doom vs. Masters of Deception; online warfare; jamming phone lines.
1984: Hacker 'Zines
Hacker magazine 2600 publication; online 'zine Phrack.

2.5 CRACKDOWN (1986-1994)

1986: Congress passes Computer Fraud and Abuse Act; crime to break into computer systems.
1 **988: The Morris Worm**
Robert T. Morris, Jr., launches self-replicating worm on Arpanet.
1989: The Germans, the KGB and Kevin Mitnick.
German Hackers arrested for breaking into U.S. computers; sold information to Soviet KGB.

Hacker "The Mentor" arrested; publishes Hacker's Manifesto.

Kevin Mitnick convicted; first person convicted under law against gaining access to interstate network for criminal purposes.

1993: Why Buy a Car When You Can Hack One? Radio station call-in contest; hacker-fugitive Kevin Paulsen and friends crack phone; they allegedly get two Porsches, $20,000 cash, vacation trips; Paulsen now a freelance journalist covering computer crime.

First Def Con hacking conference in Las Vegas

2.6 ZERO TOLERANCE (1994-1998)

1995: The Mitnick Takedown: Arrested again; charged with stealing 20,000 credits card numbers.

1995: Russian Hackers Siphon $10 million from Citibank; Vladimir Levin, leader.

Oct 1998 teenager hacks into Bell Atlantic phone system; disabled communication at airport disables runway lights.

1999 hackers attack Pentagon, MIT, FBI web sites.

1999: E-commerce Company attacked; blackmail threats followed by 8 million credit card numbers stolen.

3. HACKING

The explosive growth of the Internet has brought many good things…As with most technological advances; there is also a dark side: criminal hackers.

The term "hacker" has a dual usage in the computer industry today.

The term can be defined as:

HACKER, noun

ˆ Traditionally, a hacker is someone who likes to tinker with software or electronic systems. Hackers enjoy exploring and learning how computer systems operate. They love discovering new ways to work electronically.

ˆ Recently, hacker has taken on a new meaning — someone who maliciously breaks into systems for personal gain. Technically, these criminals are crackers (criminal hackers). Crackers break into (crack) systems with malicious intent. They are out for personal gain: fame, profit, and even revenge. They modify, delete, and steal critical information, often making other people miserable.

This complimentary description was often extended to the verb form "hacking," which was used to describe the rapid crafting of a new program or the making of changes to existing, usually complicated software. As computers became increasingly available at universities, user communities began to extend beyond researchers in engineering or computer science to other individuals who viewed the computer as a curiously flexible tool. The increasing popularity of computers and their continued high cost, access to them was usually restricted. When refused access to the computers, some users would challenge the access controls that had been put in place. They would steal passwords or account numbers by looking over someone's shoulder, explore the system for bugs that might get them past the rules, or even take control of the whole system. They would do these things in order to be able to run the programs of their choice. or just to change the limitations under which their programs were running. Initially these computer intrusions were fairly benign, with the most damage being the theft of computer time. Other times, these recreations would take the form of practical jokes. However, these intrusions did not stay benign for long. Occasionally the less talented, or less careful, intruders would accidentally bring down a system or damage its files, and the system administrators would have to restart it or make repairs. Other times, when these intruders were again denied access once their activities were discovered, they would react with purposefully destructive actions. When the number of these destructive computer intrusions became noticeable, due to the visibility of the system or the extent of the damage inflicted, it became "news" and the news media picked up on the story. Instead of using the more accurate term of "computer criminal," the media began using the term "hacker" to describe individuals who break into computers for fun, revenge, or profit. Since calling someone a "hacker" was originally meant as a compliment, computer security professionals prefer to use the term "cracker" or "intruder" for those hackers who turn to the dark side of hacking. For clarity, we will use the explicit terms "ethical hacker" and "criminal hacker" for the rest of this paper.

Old School Hackers: 1960s style Stanford or MIT hackers. Do not have malicious intent, but do have lack of concern for privacy and proprietary information. They believe the Internet was designed to be an open system.

Script Kiddies or Cyber-Punks: Nearly 12 to 30; predominantly white and male; bored in school; get caught due to bragging online; intent is to vandalize or disrupt systems.

Professional Criminals or Crackers: Make a living by breaking into systems and selling the information.

Coders and Virus Writers: See themselves as an elite; programming background and write code but won't use it themselves; have their own networks called "zoos"; leave it to others to release their code into "The Wild" or Internet.

3.1 CASE STUDY:

The Organisation

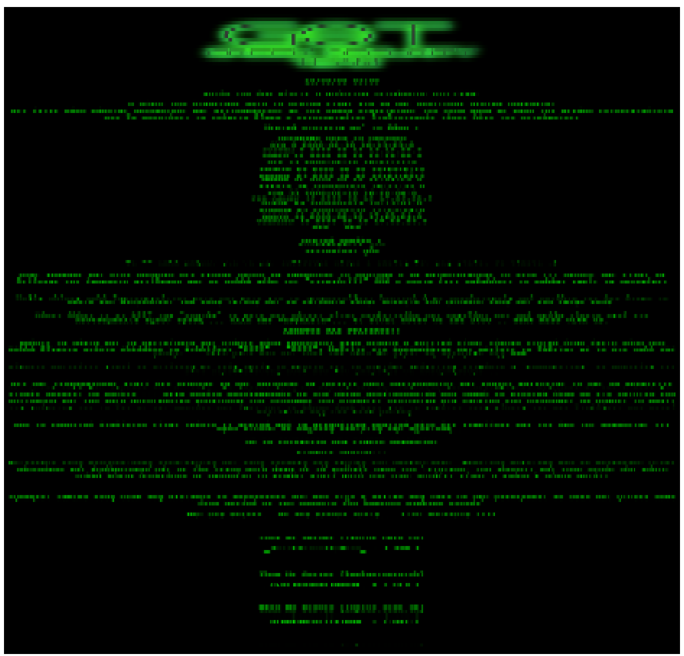
CERN, the European Organization for Nuclear Research, is one of the world's largest and most respected centres for scientific research. Its business is fundamental physics, finding out what the Universe is made of and how it works. At CERN, the world's largest and most complex scientific instruments are used to study the basic constituents of matter — the fundamental particles.

What Happened

A group of hackers identifying themselves as the 2600 succeeded in hacking into a computer network of the Large Hadron Collider at CERN. The hacker team 2600 also identified themselves as the "Greek Security Team" and was competing against a rival hacker group to successfully tap the computer system of history's largest physics experiment.

Impact

The website - cmsmon.cern.ch - can no longer be accessed by the public as a result of the attack. Scientists working at CERN, the organisation that runs the vast smasher, were worried about what the hackers could do because they were "one step away" from the computer control system of one of the huge detectors of the machine. If they had hacked into a second computer network, they could have turned off parts of the vast detector and, said the insider, "it is hard enough to make these things work if no one is messing with it." Fortunately, only one file was damaged but one of the scientists firing off emails as the CMS team fought off the hackers said it was a "scary experience".



Experiment, or CMS, one of the four "eyes" of the facility that will be analyzing the fallout of the Big Bang.

Lessons?

• Try to avoid using internet connection to the computer systems for such an important experiment. But this could not be the proper way in all sense. Hence, appointing the group of certain certified ethical hackers which can hit back such vulnerabilities.

•If you need to use the Internet for experimenting, keep it at secret level from public interference.

4. ETHICAL HACKING

With the growth of the Internet, computer security has become a major concern for businesses and governments.

In their search for a way to approach the problem, organizations came to realize that one of the best ways to evaluate the intruder threat to their interests would be to have independent computer security professionals attempt to break into their computer systems.

In the search for a way to approach the problem of hacking, organizations came to realize that one of the best ways to evaluate the intruder threat to their interests would be to have independent computer security professionals attempt to break into their computer systems. This scheme is similar to having independent auditors come into an organization to verify its bookkeeping records. In the case of computer security, these "tiger teams" or "ethical hackers" would employ the same tools and techniques as the intruders, but they would neither damage the target systems nor steal information. Instead, they would evaluate the target systems' security and report back to the owners with the vulnerabilities they found and instructions for how to remedy them. This method of evaluating the security of a system has been in use from the early days of computers. In one early ethical hack, the United States Air Force conducted a "security evaluation" of the Multics operating systems for "potential use as a two-level (secret/top secret) system." Their evaluation found that while Multics was "significantly better than other conventional systems," it also had ". . . vulnerabilities in hardware security, software security, and procedural security" that could be uncovered with "a relatively low level of effort." The authors performed their tests under a guideline of realism, so that their results would accurately represent the kinds of access that an intruder could potentially achieve. They performed tests that were simple information-gathering exercises, as well as other tests that were outright attacks upon the system that might damage its integrity. Clearly, their audience wanted to know both results. There are several other now unclassified reports that describe ethical hacking activities within the U.S. military. With the growth of computer networking, and of the Internet in particular, computer and network vulnerability studies began to appear outside of the military establishment. Most notable of these was the work by Farmer and Venema, which was originally posted to Usenet in December of 1993. They discussed publicly, perhaps for the first time, this idea of using the techniques of the hacker to assess the security of a system. With the goal of raising the overall level of security on the Internet and intranets, they proceeded to describe how they were able to gather enough information about their targets to have been able to compromise security if they had chosen to do so. They provided several specific examples of how this information could be gathered and exploited to gain control of the target, and how such an attack could be prevented. Farmer and Venema elected to share their report freely on the Internet in order that everyone could read and learn from it. However, they realized that the testing at which they had become so adept might be too complex, time-consuming, or just too boring for the typical system administrator to perform on a regular basis. For this reason, they gathered up all the tools that they had used during their work, packaged them in a single, easy-to-use application, and gave it away to anyone who chose to download it. Their program, called Security Analysis Tool for Auditing Networks, or SATAN, was met with a great amount of media attention around the world. Most of this early attention was negative, because the tool's capabilities were misunderstood. The tool was not an automated hacker program that would bore into systems and steal their secrets. Rather, the tool performed an audit that both identified the vulnerabilities of a system and provided advice on how to eliminate them. Just as banks have regular audits of their accounts and procedures, computer systems also need regular checking. The SATAN tool provided that auditing capability, but it went one step further: it also advised the user on how to correct the problems it discovered. The tool did not tell the user how the vulnerability might be exploited, because there would be no useful point in doing so.

An ethical hacker is a computer and network expert who attacks a security system on behalf of its owners, seeking vulnerabilities that a malicious hacker could exploit. To test a security system, ethical hackers use the same methods as their less principled counterparts, but report problems instead of taking advantage of them. Ethical hacking is also known as penetration testing, intrusion testing and red teaming.

"One of the best ways to evaluate the intruder threat is to have an independent computer security professionals attempt to break their computer systems"

Successful ethical hackers possess a variety of skills. First and foremost, they must be completely trustworthy. Ethical hackers typically have very strong programming and computer networking skills. They are also adept at installing and maintaining systems that use the more popular operating systems (e.g., Linux or Windows 2000) used on target systems.These base skills are augmented with detailed knowledge of the hardware and software provided by the more popular computer and networking hardware vendors.

One of the first examples of ethical hackers at work was in the 1970s, when the United States government used groups of experts called *red teams* to hack its own computer systems. According to Ed Skoudis, Vice President of Security Strategy for Predictive Systems' Global Integrity consulting practice, ethical hacking has continued to grow in an otherwise lackluster IT industry, and is becoming increasingly common outside the government and technology sectors where it began. Many large companies, such as IBM, maintain employee teams of ethical hackers.

We need protection from hacker shenanigans. An ethical hacker possesses the skills, mindset, and tools of a hacker but is also trustworthy. Ethical hackers perform the hacks as security tests for their systems. If you perform ethical hacking tests for customers or simply wants to add another certification to your credentials, you may want to consider the ethical hacker certification Certified Ethical Hacker, which is sponsored by EC Council. Ethical hacking — also known as penetration testing or white-hat hacking —involves the same tools, tricks, and techniques that hackers use, but with one major difference: Ethical hacking is legal. Ethical hacking is performed with the target's permission. The intent of ethical hacking is to discover vulnerabilities from a hacker's viewpoint so systems can be better secured. Its part of an overall information risk management program that allows for ongoing security improvements.

4.1 Understanding the Need to Hack the Systems:

To catch a thief, think like a thief. That's the basis for ethical hacking. The law of averages works against security. With the increased numbers and expanding knowledge of hackers combined with the growing number of system vulnerabilities and other unknowns, the time will come when all computer systems are hacked or compromised in some way. Protecting the systems from the bad guys — and not just the generic vulnerabilities that everyone knows about — is absolutely critical. When we know hacker tricks, we can see how vulnerable your systems are. Hacking preys on weak security practices and undisclosed vulnerabilities. Firewalls, encryption, and virtual private networks (VPN s) can create a false feeling of safety. These security systems often focus on high-level vulnerabilities, such as viruses and traffic through a firewall, without affecting how hackers work. Attacking the own systems to discover vulnerabilities is a step to making them more secure. This is the only proven method of greatly hardening our systems from attack. If we don't identify weaknesses, it's a matter of time before the vulnerabilities are exploited. As hackers expand their knowledge, so should we. We must think like them to protect our systems from them. We, as the ethical hacker, must know activities hackers carry out and how to stop their efforts. We should know what to look for and how to use that information to thwart hackers' efforts. We don't have to protect your systems from everything. We can't. The only protection against everything is to unplug our computer systems and lock them away so no one can touch them — not even us. That's not the best approach to information security. What's important is to protect our systems from known vulnerabilities and common hacker attacks. It's impossible to buttress all possible vulnerabilities on all our systems. We can't plan for all possible attacks — especially the ones that are currently unknown. However, the more combinations we can try — the more we test whole systems instead of individual units — the better our chances of discovering vulnerabilities that affect everything as a whole. Ethical Hacking makes little sense to harden our systems from unlikely attacks. For instance, if you don't have a lot of foot traffic in your office and no internal Web server running, you may not have as much to worry about as an Internet hosting provider would have. However, don't forget about insider threats from malicious employees!

4.2 Understanding the Dangers that a Systems Face

It's one thing to know that our systems generally are under fire from hackers around the world. It's another to understand specific attacks against our systems that are possible. Many information-security vulnerabilities aren't critical by themselves. However, exploiting several vulnerabilities at the same time can take its toll. For example, a default Windows OS configuration, a weak SQL Server administrator password, and a server hosted on a wireless network may not be major security concerns separately. But exploiting all three of these vulnerabilities at the same time can be a serious issue.

4.2.1.Non technical attacks:

Exploits that involve manipulating people are the greatest vulnerability within any computer or network infrastructure. Humans are trusting by nature, which can lead to social-engineering exploits. Social engineering is defined as the exploitation of the trusting nature of human beings to gain information for malicious purposes. Other common and effective attacks against information systems are physical. Hackers break into buildings, computer rooms, or other areas containing critical information or property. Physical attacks can include dumpster diving (rummaging through trash cans and dumpsters for intellectual property, passwords, network diagrams, and other information).

4.2.2 Network-infrastructure attacks:

Hacker attacks against network infrastructures can be easy, because many networks can be reached from anywhere in the world via the Internet. Here are some examples of network-infrastructure attacks:

ˆ Connecting into a network through a rogue modem attached to a computer behind a firewall

ˆ Exploiting weaknesses in network transport mechanisms, such as TCP/IP and NetBIOS

ˆ Flooding a network with too many requests, creating a denial of service (DoS) for legitimate requests

ˆ Installing a network analyzer on a network and capturing every packet that travels across it, revealing confidential information in clear text

ˆ Piggybacking onto a network through an insecure 802.11b wireless configuration

4.2.3 Operating-system attacks:

Hacking operating systems (OSs) is a preferred method of the bad guys. OSs comprises a large portion of hacker attacks simply because every computer has one and so many well-known exploits can be used against them. Occasionally, some operating systems that are more secure out of the box —such as Novell NetWare and the flavors of BSD UNIX — are attacked, and vulnerabilities turn up. But hackers prefer attacking operating systems like Windows and Linux because they are widely used and better known for their vulnerabilities. Here are some examples of attacks on operating systems:

ˆ Exploiting specific protocol implementations

ˆ Attacking built-in authentication systems

ˆ Breaking file-system security

ˆ Cracking passwords and encryption mechanisms

4.2.4. Application and other specialized attacks:

Applications take a lot of hits by hackers. Programs such as e-mail server software and Web applications often are beaten down:

ˆ Hypertext Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP) applications are frequently attacked because most firewalls and other security mechanisms are configured to allow full access to these programs from the Internet.

ˆ Malicious software (malware) includes viruses, worms, Trojan horses, and spyware. Malware clogs networks and takes down systems.

ˆ Spam (junk e-mail) is wreaking havoc on system availability and storage space. And it can carry malware. Ethical hacking helps reveal such attacks against your computer systems.

4.3 The Ethical Hacking Process

Like practically any IT or security project, ethical hacking needs to be planned in advance. Strategic and tactical issues in the ethical hacking process should be determined and agreed upon. Planning is important for any amount of testing — from a simple password-cracking test to an all-out penetration test on a Web application. Formulating the plan Approval for ethical hacking is essential. Obtaining sponsorship of the project is the first and important step. One needs someone to back up and sign off on the plan. Otherwise, the testing may be called off unexpectedly if someone claims they never authorized for the tests. The authorization can be simple. One needs a detailed plan, but that doesn't mean we have to have volumes of testing procedures. One slip can crash your systems — not necessarily what anyone wants. A well-defined scope includes the following information:
ˆ Specific systems to be tested
ˆ Risks that are involved
ˆ When the tests are performed and your overall timeline
ˆ How the tests are performed
ˆ How much knowledge of the systems you have before you start testing
ˆ What is done when a major vulnerability is discovered?
ˆ The specific deliverables — this includes security-assessment reports and a higher-level report outlining the general vulnerabilities to be addressed, along with countermeasures that should be implemented When selecting systems to test, start with the most critical or vulnerable systems.

For instance, we can test computer passwords or attempt social engineering attacks before drilling down into more detailed systems. It pays to have a contingency plan for our ethical hacking process in case something goes awry. What if we're assessing our firewall or Web application? And we take it down? This can cause system unavailability, which can reduce system performance or employee productivity. Even worse, it could cause loss of data integrity, loss of data, and bad publicity. So it is important to handle social-engineering and denial-of-service attacks carefully. Determine: how they can affect the systems we're testing and our entire organization. Determining when the tests are performed is something that we must think long and hard about. Do we test during normal business hours? How about late at night or early in the morning so that production systems aren't affected? Involve others to make sure they approve of our timing. The best approach is an unlimited attack, wherein any type of test is possible. The bad guys aren't hacking the systems within a limited scope, so why should we? Some exceptions to this approach are performing DoS, social engineering and physical-security tests. Don't stop with one security hole. This can lead to a false sense of security. Keep going to see what else you can discover. Simply pursue the path we're going down until we can't hack it any longer (pun intended). One of our goals may be to perform the tests without being detected. For example, we may be performing our tests on remote systems or on a remote office and we don't want the users to be aware of what we're doing. One don't need extensive knowledge of the systems we're testing — just a basic understanding. This will help us protect the tested systems. Understanding the systems we're testing shouldn't be difficult if we're hacking our own in-house systems. If we're hacking a customer's systems, we may have to dig deeper. Most people are scared of these assessments.

4.4 Selecting tools

As with any project, if we don't have the right tools for ethical hacking, accomplishing the task effectively is difficult. Having said that, just because we use the right tools doesn't mean that we will discover all vulnerabilities. It is important to know the personal and technical limitations. Many security-assessment tools generate false positives and negatives (incorrectly identifying vulnerabilities). Others may miss vulnerabilities. If we're performing tests such as social engineering or physical-security assessments, we may miss weaknesses. Many tools focus on specific tests, but no one tool can test for everything. For the same reason that we wouldn't drive in a nail with a screwdriver, we shouldn't use a word processor to scan our network for open ports. This is why we need a set of specific tools that we can call on for the task at hand. The more tools we have, the easier our ethical hacking efforts are. It is very much essential to make sure you that we're using the right tool for the task:
ˆ To crack passwords, we need a cracking tool such as LC4, John the Ripper or pwdump.
(A general port scanner, such as Super Scan, may not crack passwords.)
ˆ For an in-depth analysis of a Web application,
A web-application assessment tool (such as Whisker or Web Inspect) is more appropriate than a network analyzer (such as Ethereal). Hundreds, if not thousands, of tools can be used for ethical hacking — from our own words and actions to software-based vulnerability-assessment programs to hardware-based network analyzers. The following list runs down some of most favorite commercial, freeware, and open-source security tools.

4.4 Security Tools:

Foot printing and Reconnaissance : Whois, Sam Spade, Nslookup, Traceroute, Ping

Scanning and Enumeration : Nmap, NMapWin, SuperScan, IP Scanner, Hyena, Retina, LANguard

System Hacking : Telnet, Snadboy, Lophtcrack, Keylogger

Trojans and Backdoors : NetBus, SubSeven

Sniffers : Spoofing a MAC address, Spoofed Mac, Ethereal, Iris Snort

Web Based Password Cracking : Cain and Abel, Legion, Brutus

Covering Tracks : Image Hide, ClearLogs

Google Hacking and SQL Injection : Google Hacking, Google Cheat Sheet, SQL Injection

The capabilities of many security and hacking tools are often misunderstood. This misunderstanding has shed negative light on some excellent tools, such as SATAN (Security Administrator Tool for Analyzing Networks) and Nmap (Network Mapper).

Some of these tools are complex. Whichever tools we use, familiarize ourselves with them before we start using them. Thus it is quite fine to go through the following steps:
ˆ Read the readme and/or online help files for your tools.

ˆ Study the user's guide for your commercial tools.
ˆ Consider formal classroom training from the security-tool vendor or another third-party training provider, if available.

4.5 Characteristics in tools for ethical hacking

ˆ Adequate documentation.
ˆ Detailed reports on the discovered vulnerabilities, including how they may be exploited and fixed.
ˆ Updates and support when needed.
ˆ High-level reports that can be presented to managers or non techie types

These features can save our time and effort when we're executing the plan. Ethical hacking can take persistence. Time and patience are important. We should be careful when we're performing our ethical hacking tests. A hacker in our network or a seemingly benign employee looking over our shoulder may watch what's going on. This person could use this information against us. It's not practical to make sure that no hackers are on our systems before we start. Just make sure to keep everything as quiet and private as possible. This is especially critical when transmitting and storing our test results. If possible, encrypt the e-mails and files using Pretty Good Privacy (PGP) or something similar. At a minimum, password-protect them. Harness as much information as possible about the organization and systems, which is what malicious hackers do.

1. Search the Internet for your organization's name, your computer and network system names, and your IP addresses. I think "Google" is a great place to start for this.
2. Narrow the scope, targeting the specific systems which are being tested. Whether physical-security structures or Web applications, a casual assessment can turn up much information about our systems.
3. Further narrow the focus with a more critical eye. Perform actual scans and other detailed tests on the systems.
4. Perform the attacks, if that's what has been chosen to do.

4.6 Evaluating results

Assess the results to see what is uncovered, assuming that the vulnerabilities haven't been made obvious before now. I think, this is the most important step. Evaluating the results and correlating the specific vulnerabilities discovered is a skill that gets better with experience. At the end of the day we'll end up knowing our systems as well as anyone else. This makes the evaluation process much simpler moving forward.

Moving on......

When we've finished with our ethical hacking tests, we still need to implement our analysis and recommendations to make sure that our systems are secure. New security vulnerabilities continually appear. Information systems constantly change and become more complex. New hacker exploits and security vulnerabilities are regularly uncovered. Security tests are a snapshot of the security posture of our systems. At any time, everything can change, especially after software upgrades, adding computer systems, or applying patches. Plan to test regularly (for example, once a week or once a month).

5. CEH

5.1 Introduction

Attacks on the World Trade Center ignited a very important question in the hearts of the founders of EC–Council – Jay Bavisi and Haja Mohideen. Shortly after the attacks, they researched the web for "Information Security" programs that would be able to provide Information Security professionals with the necessary tools and education that will help them avert a cyber war, should the need ever arise.

The results returned from the research were disappointing and that motivated them to form the International Council of Electronic Commerce Consultants, known as the EC-Council. They soon gained the support of subject matter experts from all over the world that eventually led to the creation of various standards and certifications both in the electronic commerce and information security space. The International Council of E-Commerce Consultants (EC-Council) is a member-based organization that certifies individuals in various e-business and security skills. It is the owner and developer of the world famous Certified Ethical Hacker course, Computer Hacking Forensics Investigator program, License Penetration Tester program and various other programs offered in over 60 countries around the globe. These certifications are recognized worldwide and have received endorsements from various government agencies including the US Federal Government via the Montgomery GI Bill, and the US Government National Security Agency (NSA) and the Committee on National Security Systems (CNSS) certifying EC-Council Network Security Administrator (ENSA) program for meeting the 4011 training standard for information security professionals. Individuals who have achieved EC-Council certifications include those from some of the finest organizations around the world such as the US Army, the FBI, Microsoft, IBM and the United Nations. EC-Council has also been featured in internationally acclaimed publications including The Herald Tribune, The Wall Street Journal, The Gazette and The Economic Times as well as in online publications such as the ABC News, USA Today, The Christian Science Monitor, Boston and Gulf News.

EC-Council is the creator of the Hacker Halted conference and workshop series. The world-class Hacker Halted events are held all over the world. It had been held in Singapore, Taiwan, Mexico, Malaysia, USA and Dubai, and will be heading to many other cities in the future. Hacker Halted features renowned international speakers who are experts in the field of information security. The objective of Hacker Halted series of conferences is to raise international awareness towards increased education and ethics in information security. Another EC-Council event series is the Security Summit which is a road-show as a platform to expose individuals in the host cities of the need for information security and to help them understand the current trends and issues in information security.

5.2 Vision

EC-Council envisions itself to be a community of common interest, where individuals converge on one platform for communication, education and knowledge sharing regardless of their specific responsibilities or abilities. The organization welcomes any individual who believes in our philosophy in creating awareness and sincerely desires to enhance their skills and that of the E-commerce circle. Administration of the philosophy is done by its members in accordance to democratic principles.

5.3 Mission Statement

EC-Council aims to:

- Foster professional standards;
- Provide for communication among all E-commerce professionals, including corporate consultants in various government agencies, businesses, and education, independent consultants, and students aspiring to be E-commerce professionals;
- Provide for education through the development of curriculum, publishing of articles and books, participation in professional papers, and the sponsoring of seminars and conferences;
- Stimulate the continued growth of the E-commerce arena by providing a forum for the raising of new ideas and an effective mechanism for dialogues on these issues;
- Provide security, legal and marketing white papers in E-commerce as well as real-time updates on the current trends in the Information Security world; and
- Provide accreditation for E-commerce certifications and training programs.

5.4 Recertification:

EC-Council Continuing Education (ECE) points will serve to ensure that all EC-Council certified professionals maintain and further their knowledge. Professionals will need to meet the requirements of the ECE to avoid revocation of certification. Members holding the C|EH/CNDA designation (as well as other EC-Council certifications) will be required to re-certify under this program every three years for a minimum of 120 credits (20 credits per year).

6. CONTROVERSY

Certain computer security professionals have objected to the term ethical hacker: “There’s no such thing as an ‘ethical hacker ’ - that’s like saying ‘ethical rapist’ - it’s a contradiction in terms.” Part of the controversy may arise from the older, less stigmatized, definition of hacker, which has become synonymous with computer criminal. Some companies on the other hand do not seem to mind the association. According to EC-Council, there has been an increase of careers where CEH and other ethical hacking certifications are preferred or required.

7. ETHICAL HACKING: FUTURE IMPULSE

It is always enticed to predict the future when it comes to computer security. Of course it’s impossible to know for sure but it is possible to make an educated guess. They say we are in the “the golden age of hacking” and we do not agree more. Tools for both windows and Linux are available and now anyone can actually be a decent hacker using nothing but windows. The best of times for those curious about security and how it can be breached and the worst of times if you are sitting on the net with a vulnerable computer!

If we were to split hacking into 3 levels, say low, middle and high. Low is requiring the least amount of technical skill and relies more on social engineering and a few simple things like hardware key loggers. Middle level comprises a good skill with tools available and precompiled buffer overflows, etc... High is someone who can think way outside the box and deepest aspects of TCP/IP and can code accordingly. Our strong feeling is that the middle level as defined it will be the one that will disappear in the future. Buffer overflows will become a thing of the past. Technology is growing strongly towards that direction. Exploiting code will slowly become more and more difficult and tools that focus on that will lose more and more of their effectiveness. Hackers will either focus on things like social engineering or gaining physical access. Join a cleaning crew and place a hardware key logger. Come back the next night and retrieve it and while not very sophisticated it can be very devastating none the less. The high end will be those that understand the very core of IP6 and will understand how to manipulate packet flows in ways no one has ever thought about. Obviously if this scenario is correct, most hackers will focus on the low level and that perhaps is even scarier. Using a combination of hardware and social skills could prove the most difficult to defend against.

That’s the future as I see it happening. Let’s wait and see!

8. CONCLUSION:

The idea of testing the security of a system by trying to break into it is not new.

From a practical standpoint the security problem will remain as long as manufacturers remain committed to current system architectures, produced without a firm requirement for security. As long as there is support for ad hoc fixes and security packages for these inadequate designs and as long as the illusory results of penetration teams are accepted as demonstrations of a computer system security, proper security will not be a reality. Regular auditing, vigilant intrusion detection, good system administration practice, and computer security awareness are all essential parts of an organization’s security efforts. A single failure in any of these areas could very well expose an organization to cyber-vandalism, embarrassment, loss of revenue or mind share, or worse. Any new technology has its benefits and its risks. While ethical hackers can help clients better understand their security needs, it is up to the clients to keep their guards in place.

9. ACKNOWLEDGMENTS

We would like to thank several people: who really helped us in this effort Dr.V.Ghodki, Professor of computer sciences and applications, for sharing their amazing expertise and their ability to make just about anyone understand more about security; Chinmay and Bushan for their encyclpedia knowledge of computer security research and for his amazing ability to produce copies of every notable paper on the subject that was ever published.

10. REFERENCES

[1] Ethical Hacking by C. C. Palmar ;IBM research division

[2] Ethical Hacking and corporate security by Ankit Fadia

[3] Ethical Hacking by R. Hartley

[4] IEEE journals and proceeding papers

[5] The first use of the term “ethical hackers” appears to have been in an interview with John Patrick of IBM by Gary that appeared in a June 1995 issue of ComputerWorld.

[6] wikipedia

[7] http://www.faqs.org/usenet/.

[8] http://www.cs.ruu.nl/cert-uu/satan.html.