Ethical Hacking Basics Class part 1

Introduction

This lesson introduces you to the world of ethical hacking. Ethical hacking is a form of legal hacking that is done with the permission of an organization to help increase its security. This lesson discusses many of the business aspects of penetration (pen) testing. Information about how to perform a pen test, what types can be performed, what are the legal requirements, and what type of report should be delivered are all basic items that you will need to know before you perform any type of security testing. However, first, you need to review some security basics. This lesson starts with a discussion of confidentiality, integrity, and availability. Finally, the lesson finishes up with the history of hacking and a discussion of some of the pertinent laws.

NOTE

Nothing learned in this class is intended to teach or encourage the use of security tools or methodologies for illegal or unethical purposes. Always act in a responsible manner. Make sure that you have written permission from the proper individuals before you use any of the tools or techniques described within. Always obtain permission before installing any of these tools on a network.

Security Fundamentals

Security is about finding a balance, as all systems have limits. No one person or company has unlimited funds to secure everything, and we cannot always take the most secure approach. One way to secure a system from network attack is to unplug it and make it a standalone system. Although this system would be relatively secure from Internet-based attackers, its usability would be substantially reduced. The opposite approach of plugging it in directly to the Internet without any firewall, antivirus, or security patches would make it extremely vulnerable, yet highly accessible. So, here again, you see that the job of security professionals is to find a balance somewhere between security and usability. Figure 1.1 demonstrates this concept.

To find this balance, you need to know what the goals of the organization are, what

security is, and how to measure the threats to security. The next section discusses the goals of security.

Goals of Security

Objective:

Understand the security triangle, also known as CIA (confidentiality, integrity, and availability).

There are many ways in which security can be achieved, but it's universally agreed that the security triad of confidentiality, integrity, and availability (CIA) form the basic building blocks of any good security initiative.

Confidentiality addresses the secrecy and privacy of information. Physical examples of confidentiality include locked doors, armed guards, and fences. Logical examples of confidentiality can be seen in passwords, encryption, and firewalls. In the logical world, confidentiality must protect data in storage and in transit. For a real-life example of the failure of confidentiality, look no further than the recent news reports that have exposed how several large-scale breaches in confidentiality were the result of corporations, such as Time Warner and City National Bank, misplacing or losing backup tapes with customer accounts, names, and credit information. The simple act of encrypting thebackup tapes could have prevented or mitigated the damage.

Integrity is the second piece of the CIA security triad. Integrity provides for the correctness of information. It allows users of information to have confidence in its correctness. Correctness doesn't mean that the data is accurate, just that it hasn't been modified in storage or transit. Integrity can apply to paper or electronic documents. It is much easier to verify the integrity of a paper document than an electronic one. Integrity in electronic documents and data is much more difficult to protect than in paper ones. Integrity must be protected in two modes: storage and transit.

Information in storage can be protected if you use access and audit controls. Cryptography can also protect information in storage through the use of hashing algorithms. Real-life examples of this technology can be seen in programs such as Tripwire, MD5Sum, and Windows File Protection (WFP). Integrity in transit can be ensured primarily by the protocols used to transport the data. These security

controls include hashing and cryptography.

Availability is the third leg of the CIA triad. Availability simply means that when a legitimate user needs the information, it should be available. As an example, access to a backup facility 24x7 does not help if there are no updated backups from which to restore. Backups are one of the ways that availability is ensured. Backups provide a copy of critical information should files and data be destroyed or equipment fail. Failover equipment is another way to ensure availability. Systems such as redundant array of inexpensive disks (RAID) and subscription services such as redundant sites (hot, cold, and warm) are two other examples. Disaster recovery is tied closely to availability, as it's all about getting critical systems up and running quickly. Denial of service (DoS) is an attack against availability. Although these attacks might not give access to the attacker, they dodeny legitimate users the access they require.

Assets, Threats, and Vulnerabilities

Objectives:

Recall essential terminology
List the elements of security

As with any new technology topic, terminology is used that must be learned to better understand the field. To be a security professional, you need to understand the relationship between threats, assets, and vulnerabilities.

Risk is the probability or likelihood of the occurrence or realization of a threat. There are three basic elements of risk: assets, threats, and vulnerabilities. Let's discuss each of these.

An asset is any item of economic value owned by an individual or corporation. Assets can be real — such as routers, servers, hard drives, and laptops — or assets can be virtual, such as formulas, databases, spreadsheets, trade secrets, and processing time. Regardless of the type of asset discussed, if the asset is lost, damaged, or compromised, there can be an economic cost to the organization.

A threat is any agent, condition, or circumstance that could potentially cause harm, loss, damage, or compromise to an IT asset or data asset. From a security professional's perspective, threats can be categorized as events that can affect the

confidentiality, integrity, or availability of the organization's assets. These threats can result in destruction, disclosure, modification, corruption of data, or denial of service. Some examples of the types of threats an organization can face include the following:

Unauthorized Access

If userids and passwords to the organization's infrastructure are obtained and confidential information is compromised and unauthorized, access is granted to the unauthorized user who obtained the userids and passwords.

Stolen/Lost/Damaged/Modified Data

A critical threat can occur if the information is lost, damaged, or unavailable to legitimate users.

Disclosure of Confidential Information

Anytimethere is a disclosure of confidential information, it can be a critical threat to an organization if that disclosure causes loss of revenue, causes potential liabilities, or provides a competitive advantage to an adversary.

Hacker Attacks

An insider or outsider who is unauthorized and purposely attacks an organization's components, systems, or data.

Cyber Terrorism

Attackers whotarget critical, national infrastructures such as water plants, electric plants, gas plants, oil refineries, gasoline refineries, nuclear power plants, waste management plants, and so on.

Viruses and Malware

An entirecategory of software tools that are malicious and are designed to damage or destroy a system or data.

Denial of Service (DoS) or Distributed Denial of Service Attacks

An attack against availability that isdesigned to bring the network and/or access to a particular TCP/IP host/server to its knees by flooding it with useless traffic. Many DoSattacks, such as the Ping of Death and Teardrop, exploit limitations in the

TCP/IP protocols. Like malware, hackers constantly develop new DoS attacks, so they form a continuous threat.

Natural Disasters, Weather, or Catastrophic Damage

Hurricanes, such as Katrina that hit New Orleans in 2005, storms, weather outages, fire, flood, earthquakes, and other natural events compose an ongoing threat.

If the organization is vulnerable to any of these threats, there is an increased risk of successful attack.

A vulnerability is a weakness in the system design, implementation, software or code, or the lack of a mechanism. A specific vulnerability might manifest as anything from a weakness in system design to the implementation of an operational procedure. Vulnerabilities might be eliminated or reduced by the correct implementation of safeguards and security countermeasures.

Vulnerabilities and weaknesses are common with software mainly because there isn't any perfect software or code in existence. Vulnerabilities in software can be found in each of the following:

Firmware

This software is usually stored in ROM and loaded during system power up.

Operating System

This operating system software is loaded in workstations and servers.

Configuration Files

The configuration file and configuration setup for the device.

Application Software

The application or executable file that is run on a workstation or server.

Software Patch

This is a small piece of software or code snippet that the vendor or developer of the software typically releases as software updates, software maintenance, and known software vulnerabilities or weaknesses.

Vulnerabilities are not the only concern the ethical hacker will have. Exploits are a big concern, as they are a common mechanism used to gain access. That's discussed next.

Defining an Exploit

An exploit refers to a piece of software, tool, or technique that takes advantage of a vulnerability that leads to privilege escalation, loss of integrity, or denial of service on a computer system. Exploits are dangerous because all software has vulnerabilities; hackers and perpetrators know that there are vulnerabilities and seek to take advantage of them. Although most organizations attempt to find and fix vulnerabilities, some organizations lack sufficient funds for securing their networks. Even those that do are burdened with the fact that there is a window between when a vulnerability is discovered and when a patch is available to prevent the exploit. The more critical the server, the slower it is typically patched. Management might be afraid of interrupting the server or afraid that the patch might affect stability or performance. Finally, the time required to deploy and install the software patch on production servers and workstations exposes an organization's IT infrastructure to an additional period of risk.

Security Testing

Objective:

Define the modes of ethical hacking
Security testing is the primary job of ethical hackers. These tests might be configured in such way that the ethical hackers have no knowledge, full knowledge, or partial knowledge of the target of evaluation (TOE).

NOTE

The term target of evaluation (TOE) is widely used to identify an IT product or system that is the subject of an evaluation. The EC-Council and some security guidelines and standards use the term to describe systems that are being tested to measure their confidentiality, integrity, and availability.

The goal of the security test (regardless of type) is for the ethical hacker to test the security system and evaluate and measure its potential vulnerabilities.

No Knowledge Tests (Blackbox)

No knowledge testing is also known as blackbox testing. Simply stated, the security team has no knowledge of the target network or its systems. Blackbox testing simulates an outsider attack as outsiders usually don't know anything about the

network or systems they are probing. The attacker must gather all types of information about the target to begin to profile its strengths and weaknesses. The advantages of blackbox testing include

The test is unbiased as the designer and the tester are independent of each other. The tester has no prior knowledge of the network or target being examined. Therefore there are no preset thoughts or ideas about the function of the network. A wide range of resonances work and are typically done to footprint the organization, which can help identify information leakage. The test examines the target in much the same way as an external attacker.

The disadvantages of blackbox testing include
It can take more time to perform the security tests.
It is usually more expensive as it takes more time to perform.
It focuses only on what external attackers see, while in reality, most attacks are launched by insiders.

Full Knowledge Testing (Whitebox)

Whitebox testing takes the opposite approach of blackbox testing. This form of security test takes the premise that the security tester has full knowledge of the network, systems, and infrastructure. This information allows the security tester to follow a more structured approach and not only review the information that has been provided but also verify its accuracy. So, although blackbox testing will typically spend more time gathering information, whitebox testing will spend that time probing for vulnerabilities.

Partial Knowledge Testing (Graybox)

In the world of software testing, graybox testing is described as a partial knowledge test. EC-Council literature describes graybox testing as a form of internal test. Therefore, the goal is to determine what insiders can access. This form of test might also prove useful to the organization as so many attacks are launched by insiders.

Types of Security Tests

Objective:

State security testing methodologies

Several different types of security tests can be performed. These can range from those that merely examine policy to those that attempt to hack in from the Internet and mimic the activities of true hackers. These security tests are also known by many names, including

Vulnerability Testing
Network Evaluations
Red Team Exercises
Penetration Testing
Host Vulnerability Assessment
Vulnerability Assessment
Ethical Hacking

No matter what the security test is called, it is carried out to make a systematic examination of an organization's network, policies, and security controls. Its purpose is to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of potential security measures, and confirm the adequacy of such measures after implementation. Security tests can be defined as one of three types, which include highlevel assessments, network evaluations, and penetration tests. Each is described as follows:

High-level assessments

Also called a level I assessment, it is a top-down look at the organization's policies, procedures, and guidelines. This type of vulnerability assessment does not include any hands-on testing. The purpose of a top-down assessment is to answer three questions: Do the applicable policies exist?

Are they being followed?
Is there content sufficient to guard against potential risk?

Network evaluations

Also called a level II assessment, it has all the elements specified in a level I assessment plus includes hands-on activities. These hands-on activities would include information gathering, scanning, vulnerability assessment scanning, and other hands-on activities. Throughout this book, tools and techniques used to perform this type of assessment are discussed.

Penetration tests

Unlike assessments and evaluations, penetration tests are adversarial in nature. Penetration tests are also referred to as level III assessments. These events typically take on an adversarial role and look to see what the outsider can access and control. Penetration tests are less concerned with policies and procedures and are more focused on finding low hanging fruit and seeing what a hacker can accomplish on this network.

NOTE

Just remember that penetration tests are not fully effective if an organization does not have the policies and procedures in place to control security. Without adequate policies and procedures, it's almost impossible to implement real security. Documented controls are required.

How do ethical hackers play a role in these tests? That's the topic of the next section.

Hacker and Cracker Descriptions

Objective:

Discuss malicious hackers

To understand your role as an ethical hacker, it is important to know the players. Originally, the term hacker was used for a computer enthusiast. A hacker was a person who enjoyed understanding the internal workings of a system, computer, and computer network. Over time, the popular press began to describe hackers as individuals who broke into computers with malicious intent. The industry responded by developing the word cracker, which is short for criminal hacker. The term cracker was developed to describe individuals who seek to compromise the security of a system without permission from an authorized party. With all this confusion over how

to distinguish the good guys from the bad guys, the term ethical hacker was coined. An ethical hacker is an individual who performs security tests and other vulnerability assessment activities to help organizations secure their infrastructures. Sometimes ethical hackers are referred to as White Hat Hackers.

Hacker motives and intentions vary. Some hackers are strictly legitimate, whereas others routinely break the law. Let's look at some common categories:

Whitehat Hackers

These individuals perform ethical hacking to help secure companies and organizations. Their belief is that you must examine your network in the same manner as a criminal hacker to better understand its vulnerabilities. Reformed Blackhat Hackers — These individuals often claim to have changed their ways and that they can bring special insight into the ethical hacking methodology.

Grayhat Hackers —

These individuals typically follow the law but sometimes venture over to the darker side of blackhat hacking. It would be unethical to employ these individuals to perform security duties for your organization as you are never quite clear where they stand.

Who Attackers Are
Ethical hackers are up against several individuals in the battle to secure the network. The following list presents some of the more commonly used terms for these attackers:

Phreakers —

The original hackers. These individuals hacked telecommunication and PBX systems to explore the capabilities and make free phone calls. Their activities include physical theft, stolen calling cards, access to telecommunication services, reprogramming of telecommunications equipment, and compromising userids and passwords to gain unauthorized use of facilities, such as phone systems and voice mail.

Script/Click Kiddies —

A term used to describe often younger attackers who use widely available freeware vulnerability assessment tools and hacking tools that are designed for attacking purposes only. These attackers typically do not have any programming or hacking

skills and, given the techniques used by most of these tools, can be defended against with the proper security controls and risk mitigation strategies.

Disgruntled Employee —

Employees who have lost respect and integrity for the employer. These individuals might or might not have more skills than the script kiddie. Many times, their rage and anger blind them. They rank as a potentially high risk because they have insider status, especially if access rights and privileges were provided or managed by the individual.

Whackers —

Whackers are typically newbies who focus their limited skills and abilities on attacking wireless LANs and WANs.

Software Cracker/Hacker —

Individualswho have skills in reverse engineering software programs and, in particular, licensing registration keys used by software vendors when installing software onto workstations or servers. Although many individuals are eager to partake of their services, anyone who downloads programs with cracked registration keys are breaking the law and can be a greater potential risk and subject to malicious code and malicious software threats that might have been injected into the code.

Cyber-Terrorists/Cyber-Criminals

An increasing category of threat that can be used to describe individuals or groups of individuals who are typically funded to conduct clandestine or espionage activities on governments, corporations, and individuals in an unlawful manner. These individuals are typically engaged in sponsored acts of defacement; DoS/DDoS attacks identify theft, financial theft, or worse, compromising critical infrastructures in countries, such as nuclear power plants, electric plants, water plants, and so on.

System Cracker/Hacker —

Elite hackers who have specific expertise in attacking vulnerabilities of systems and networks by targeting operating systems. These individuals get the most attention and media coverage because of the globally affected viruses, worms, and Trojans that are created by System Crackers/Hackers. System Crackers/Hackers perform

interactive probing activities to exploit security defects and security flaws in network operating systems and protocols.

Now that you have an idea who the legitimate security professionals are up against, let's briefly discuss some of the better known crackers and hackers.

Hacker and Cracker History

The well-known hackers of today grew out of the phone phreaking activities of the 1960s. In 1969, Mark Bernay, also known as "The Midnight Skulker," wrote a computer program that allowed him to read everyone else's ID and password at the organization where he worked. Although he was eventually fired, no charges were ever filed, as computer crime was so new, there were no laws against it.

Computer innovators include:

Steve Wozniak and Steve Jobs —

Members of the Homebrew Computer Club of Palo Alto. John Draper was also a member of this early computer club. Wozniak and Jobs went on to become co-founders of Apple Computer.

Dennis Ritchie and Ken Thompson —

While not criminal hackers, their desire for discovery led to the development of UNIX in 1969 while working at Bell Labs.

Well-known hackers and phreakers include:

John Draper —

Dubbed "Captain Crunch" for finding that a toy whistle shipped in boxes of Captain Crunch cereal had the same frequency as the trunking signal of AT&T, 2,600Hz. This discovery was made with the help of Joe Engressia. Although Joe was blind, he could whistle into a phone and produce a perfect 2,600Hz frequency. This tone was useful for placing free long distance phone calls.

Mark Abene —

Known as Phiber Optik. Mark helped form the "Masters of Deception" in 1990. Before being arrested in 1992, they fought an extended battle with "Legion of Doom."

Kevin Poulsen —

Known asDark Dante. Kevin took over all phones in Los Angeles in 1990 to ensure victory in a phone “call-in contest,” for a Porsche 944. He was later arrested.

Robert Morris —

The son of a chief scientist at the NSA. Morris accidentally released the “Morris Worm” in 1988 from a Cornell University lab. This is now widely seen as the first release of a worm onto the Internet.

Kevin Mitnick —

Known as “Condor,” Mitnick was the first hacker to hit the FBI Most Wanted list. Broke into such organizations as Digital Equipment Corp., Motorola, Nokia Mobile Phones, Fujitsu, and others. He was arrested in 1994 and has now been released and works as a legitimate security consultant.

Vladimir Levin —

A Russian hacker who led a team of hackers who siphoned off $10 million from Citibank and transferred the money to bank accounts around the world. Levin eventually stood trial in the United States and was sentenced to three years in prison. Authorities recovered all but $400,000.00 of the stolen money.

Adrian Lamo —

Known asthe “Homeless Hacker” because of his transient lifestyle. Lamo spent his days squatting in abandoned buildings and traveling to Internet cafes, libraries, and universities to exploit security weaknesses in high-profile company networks, such as Microsoft, NBC, and the New York Times. He was eventually fined and prosecuted for the New York Times hack.

Although this list does not include all the hackers, crackers, and innovators of the computer field, it should give you an idea of some of the people who have made a name for themselves in this industry. Let’s now talk more about ethical hackers.

Ethical Hackers

Objective:

Define ethical hacking

Ethical hackers perform penetration tests. They perform the same activities a hacker would but without malicious intent. They must work closely with the host organization to understand what the organization is trying to protect, who they are trying to protect these assets from, and how much money and resources the organization is willing to expend to protect the assets.

By following a methodology similar to that of an attacker, ethical hackers seek to see what type of public information is available about the organization. Information leakage can reveal critical details about an organization, such as its structure, assets, and defensive mechanisms. After the ethical hacker gathers this information, it will be evaluated to determine whether it poses any potential risk. The ethical hacker further probes the network at this point to test for any unseen weaknesses.

Penetration tests are sometimes performed in a double blind environment. This means that the internal security team has not been informed of the penetration test. This serves as an important purpose, allowing management to gauge the security team's responses to the ethical hacker's probing and scanning. Do they notice the probes or have the attempted attacks gone unnoticed? Now that the activities performed by ethical hackers have been described, let's spend some time discussing the skills that ethical hackers need, the different types of security tests that ethical hackers perform, and the ethical hacker rules of engagement.

Required Skills of an Ethical Hacker

Objective:

Describe ethical hackers and their duties

Ethical hackers need hands-on security skills. Although you do not have to be an expert in everything, you should have an area of expertise. Security tests are typically performed by teams of individuals, where each individual typically has a core area of expertise. These skills include:

Routers —

Knowledgeof routers, routing protocols, and access control lists (ACLs). Certifications such a Cisco Certified Network Associate (CCNA) or Cisco Certified Internetworking Expert (CCIE) can be helpful.

Microsoft —

Skills in the operation, configuration, and management of Microsoft-based systems. These can run the gamut from Windows NT to Windows 2003. These individuals might be Microsoft Certified Administrator (MCSA) or Microsoft Certified Security Engineer (MCSE) certified.

Linux —

A good understanding of the Linux/UNIX OS. This includes security setting, configuration, and services such as Apache. These individuals may be Red Hat, or Linux+ certified.

Firewalls —

Knowledge of firewall configuration and the operation of intrusion detection systems (IDS) and intrusion prevention systems (IPS) can be helpful when performing a security test. Individuals with these skills may be certified in Cisco Certified Security Professional (CCSP) or Checkpoint Certified Security Administrator (CCSA).

Mainframes —

Although mainframes do not hold the position of dominance they once had in business, they still are widely used. If the organization being assessed has mainframes, the security teams would benefit from having someone with that skill set on the team.

Network protocols —

Most modern networks are Transmission Control Protocol/ Internet Protocol (TCP/IP), although you might still find the occasional network that uses Novell or Apple routing information. Someone with good knowledge of networking protocols, as well as how these protocols function and can be manipulated, can play a key role in the team. These individuals may possess certifications in other OSes, hardware, or even posses a Network+ or Security+ certification.

Project management —

Someone will have to lead the security test team, and if you are chosen to be that person, you will need a variety of the skills and knowledge types listed previously. It can also be helpful to have good project management skills. After all, you will be leading, planning, organizing, and controlling the penetration test team. Individuals in this role may benefit from having Project Management Professional (PMP) certification.

On top of all this, ethical hackers need to have good report writing skills and must always try to stay abreast of current exploits, vulnerabilities, and emerging threats as their goals are to stay a step ahead of malicious hackers.

Modes of Ethical Hacking

With all this talk of the skills that an ethical hacker must have, you might be wondering how the ethical hacker can put these skills to use. An organization's IT infrastructure can be probed, analyzed, and attacked in a variety of ways. Some of the most common modes of ethical hacking are shown here:

Insider attack —

This ethical hack simulates the types of attacks and activities that could be carried out by an authorized individual with a legitimate connection to the organization's network.

Outsider attack —

This ethical hack seeks to simulate the types of attacks that could be launched across the Internet. It could target Hypertext Transfer Protocol (HTTP), Simple Mail Transfer Protocol (SMTP), Structured Query Language (SQL), or any other available service.

Stolen equipment attack —

This simulation is closely related to a physical attack as it targets the organization's equipment. It could seek to target the CEO's laptop or the organization's backup tapes. No matter what the target, the goal is the same — extract critical information, usernames, and passwords.

Physical entry —

This simulationseeks to test the organization's physical controls. Systems such as doors, gates, locks, guards, closed circuit television (CCTV), and alarms are tested to see whether they can be bypassed.

Bypassed authentication attack —

This simulation is tasked with looking for wireless access points (WAP) and modems. The goal is to see whether these systems are secure and offer sufficient authentication controls. If the controls can be bypassed, the ethical hacker might probe to see what level of system control can be obtained.

Social engineering attack —

This simulation does not target technical systems or physical access. Social engineering attacks target the organization's employees and seek to manipulate them to gain privileged information. Proper controls, policies, and procedures can go a long way in defeating this form of attack.

Rules of Engagement —

Every ethical hacker must abide by a few simple rules when performing the tests described previously. If not, bad things can happen to you, which might include loss of job, civil penalty, or even jail time.

Never exceed the limits of your authorization —

Every assignment will have rules of engagement. These not only include what you are authorized to target, but also the extent that you are authorized to control such system. If you are only authorized to obtain a prompt on the target system, downloading passwords and starting a crack on these passwords would be in excess of what you have been authorized to do.

The tester should protect himself by setting up limitation as far as damage is concerned. There has to be an NDA between the client and the tester to protect them both. There is a good example of a get out of jail document at

HYPERLINK "http://www.professionalsecuritytesters.org/modules.php?name=Downloads&d_op=viewdownload&cid=1 "http://www.professionalsecurityteste...download&cid=1

Be ethical —

That's right; the big difference between a hacker and an ethical hacker is the word ethics. Ethics is a set of moral principles about what is correct or the right thing to do. Ethical standards are sometimes different from legal standards in that laws define what we must do, whereas ethics define what we should do.

The OSSTMM — An Open Methodology

In December 2001, the Open Source Security Testing Methodology Manual (OSSTMM) began. Hundreds of people contributed knowledge, experience, and peer-review to the project. Eventually, as the only publicly available methodology that tested security from the bottom of operations and up (as opposed to from the policy on down), it received the attention of businesses, government agencies, and militaries around the world. It also scored success with little security startups and independent ethical hackers who wanted a public source for client assurance of their security testing services. The primary purpose of the OSSTMM is to provide a scientific methodology for the accurate characterization of security through examination and correlation in a consistent and reliable way. Great effort has been put into the OSSTMM to assure reliable cross-reference to current security management methodologies, tools, and resources. This manual is adaptable to penetration tests, ethical hacking, security assessments, vulnerability assessments, red-teaming, blue-teaming, posture assessments, and security audits. Your primary purpose for using it should be to guarantee facts and factual responses, which in turn assures your integrity as a tester and the organization you are working for, if any. The end result is a strong, focused security test with clear and concise reporting.www.isecom.org is the main site for the nonprofit organization, ISECOM, maintaining the OSSTMM and many other projects. This “in the field” segment was contributed by Pete Herzog, Managing Director, ISECOM.

Maintain confidentiality —

During security evaluations, you will likely be exposed to many types of confidential information. You have both a legal and moral standard to treat this information with the utmost privacy. This information should not be shared with third parties and should not be used by you for any unapproved purposes. There is an obligation to protect the information sent between the tester and the client. This has to be specified in the agreement.

Do no harm —

It’s ofutmost importance that you do no harm to the systems you test. Again, a major difference between a hacker and an ethical hacker is that you should do no harm. Misused, security tools can lock out critical accounts, cause denial of service (DoS), and crash critical servers or applications. Care should be taken to prevent these events unless that is the goal of the test.

Test Plans — Keeping It Legal

Most of us probably make plans before we take a big trip or vacation. We think about what we want to see, how we plan to spend our time, what activities are

available, and how much money we can spend and not regret it when the next credit card bill arrives. Ethical hacking is much the same minus the credit card bill. Many details need to be worked out before a single test is performed. If you or your boss is tasked with managing this project, some basic questions need to be answered, such as what's the scope of the assessment, what are the driving events, what are the goals of the assessment, what will it take to get approval, and what's needed in the final report.

Before an ethical hack test can begin, the scope of the engagement must be determined.

Defining the scope of the assessment is one of the most important parts of the ethical hacking process. At some point, you will be meeting with management to start the discussions of the how and why of the ethical hack. Before this meeting ever begins, you will probably have some idea what management expects this security test to accomplish. Companies that decide to perform ethical hacking activities don't do so in a vacuum. You need to understand the business reasons behind this event. Companies can decide to perform these tests for various reasons.

Some of the most common reasons are listed as follows:

A breach in security - One or more events has occurred that has highlighted a lapse in security. It could be that an insider was able to access data that should have been unavailable to him, or it could be that an outsider was able to hack the organization's web server.

Compliance with state, federal, regulatory, or other law or mandate — Compliance with state or federal laws is another event that might be driving the assessment. Companies can face huge fines and potential jail time if they fail to comply with state and federal laws. The Gramm-Leach-Bliley Act (GLBA), Sarbanes-Oxley (SOX), and Health Insurance Portability and Accountability Act (HIPAA) are three such laws. HIPAA requires organizations to perform a vulnerability assessment. Your organization might decide to include ethical hacking into this test regime.

NOTE

One such standard that the organization might be attempting to comply with is ISO 17799. This information security standard was first published in December 2000 by the International Organization for Standardization and the International Electrotechnical Commission. This code of practice for information security management is considered a security standard benchmark.

. Security Policy
. Security Organization
. Asset Control and Classification

. Environmental and Physical Security
. Employee Security
. Computer and Network Management
. Access Controls
. System Development and Maintenance
. Business Continuity Planning
. Compliance

Due diligence — Due diligence is another one of the reasons a company might decide to perform a penetration test. The new CEO might want to know how good the organization's security systems really are, or it could be that the company is scheduled to go through a merger or is acquiring a new firm. If so, the penetration test might occur before the purchase or after the event. These assessments are usually going to be held to a strict timeline. There is only a limited amount of time before the purchase and if performed afterward, the organization will probably be in a hurry to integrate the two networks as soon as possible.

Test Phases

Security assessments in which ethical hacking activities will take place are composed of three phases. These include the scoping of the assessment in which goals and guidelines are established, performing the assessment, and performing post assessment activities. The post assessment activities are when the report and remediation activities would occur. Figure 1.2 shows the three phases of the assessment and their typical times.

Establishing Goals

The need to establish goals is also critical. Although you might be ready to jump in and begin hacking, a good plan will detail the goals and objectives of the test. Some common goals include system certification and accreditation, verification of policy compliance, and proof that the IT infrastructure has the capability to defend against technical attacks.

Are the goals to certify and accredit the systems being tested? Certification is a technical evaluation of the system that can be carried out by independent security teams or by the existing staff. Its goal is to uncover any vulnerabilities or weaknesses in the implementation. Your goal will be to test these systems to make sure that they are configured and operating as expected, that they are connected to and communicate with other systems in a secure and controlled manner, and that they handle data in a secure and approved manner.

If the goals of the penetration test are to determine whether current policies are being followed, the test methods and goals might be somewhat different. The security team will be looking at the controls implemented to protect information being

stored, being transmitted, or being processed. This type of security test might not have as much hands-on hacking, but might use more social engineering techniques and testing of physical controls. You might even direct one of the team members to perform a little dumpster diving.

The goal of a technical attack might be to see what an insider or outsider can access. Your goal might be to gather information as an outsider and then use that data to launch an attack against a web server or externally accessible system.

Regardless of what type of test you are asked to perform, there are some basic questions you can ask to help establish the goals and objectives of the tests. These include the following:

What is the organization's mission?
What specific outcomes does the organization expect?
What is the budget?
When will tests be performed — during work hours, after hours, or weekends?
How much time will the organization commit to completing the security evaluation?
Will insiders be notified?
Will customers be notified?
How far will the test proceed? Root the box, gain a prompt, or attempt to retrieve another prize, such as the CEO's password.
Who do you contact should something go wrong?
What are the deliverables?
What outcome is management seeking from these tests?

Getting Approval

Getting approval is a critical event in the testing process. Before any testing actually begins, you need to make sure that you have a plan that has been approved in writing. If this is not done, you and your team might face unpleasant consequences, which might include being fired or even criminal charges.

TIP

Written approval is the most critical step of the testing process. You should never perform any tests without written approval.

If you are an independent consultant, you might also get insurance before starting any type of test. Umbrella policies and those that cover errors and omissions are commonly used. These types of liability policies can help protect you should anything go wrong. To help make sure that the approval process goes smoothly, you should make sure that someone is the champion of this project. This champion or project sponsor is the lead contact to upper management and your contact person. Project sponsors can be instrumental in helping you gain permission to begin testing

and also to provide you with thefunding and materials needed to make this a success.

NOTE

Management support is critical in a security test to be successful (or in Kartik and Travis' case, from being expeled).

Ethical Hacking Report

Objective:

Describe test deliverables

Although we have not actually begun testing, you do need to start thinking about the final report. Throughout the entire process, you should be in close contact with management to keep them abreast of your findings. There shouldn't be any big surprises when you submit the report. While you might have found some serious problems, they should be discussed with management before the report is written and submitted. The goal is to keep them in the loop and advised of the status of the assessment. If you find items that present a critical vulnerability, you should stop all tests and immediately inform management. Your priority should always be the health and welfare of the organization.

The report itself should detail the results of what was found. Vulnerabilities should be discussed as should the potential risk they pose. Although people aren't fired for being poor report writers, don't expect to be promoted or praised for your technical findings if the report doesn't communicate your findings clearly. The report should present the results of the assessment in an easy, understandable, and fully traceable way. The report should be comprehensive and self-contained. Most reports contain the following sections:

Introduction
Statement of work performed
Results and conclusions
Recommendations

Since most companies are not made of money and cannot secure everything, you should rank your recommendations so that the ones with the highest risk/highest probability are at the top of the list.

The report needs to be adequately secured while in electronic storage. Encryption should be used. The printed copy of the report should be marked “Confidential” and while in its printed form, care should be taken to protect the report from unauthorized individuals. You have an ongoing responsibility to ensure the safety of the report and all information gathered. Most consultants destroy reports and all test information after a contractually obligated period of time.

TIP

The report is a piece of highly sensitive material and should be protected in storage and when in printed form.

Ethics and Legality

Objective:

Know the laws dealing with computer crimes and their implications Recent FBI reports on computer crime indicate that unauthorized computer use in 2005 was reported at 56 percent of U.S. companies surveyed. This is an increase of 3 percent from 2004. Various website attacks were up 6 percent from 2004. These figures indicate that computer crime caused by hackers continues to increase. A computer or network can become the victim of a crime committed by a hacker. Hackers use computers as a tool to commit a crime or to plan, track, and control a crime against other computers or networks. Your job as an ethical hacker is to find vulnerabilities before the attackers do and help prevent them from carrying out malicious activities. Tracking and prosecuting hackers can be a difficult job as international law is often ill-suited to deal with the problem. Unlike conventional crimes that occur in one location, hacking crimes might originate in India, use a system based in Singapore, and target a computer network located in Canada. Each country has conflicting views on what constitutes cyber crime. Even if hackers can be punished, attempting to do so can be a legal nightmare. It is hard to apply national borders to a medium such as the Internet that is essentially borderless.

NOTE

Some individuals approach computing and hacking from the social perspective and believe that hacking can promote change. These individuals are known as hactivists,

these “hacker activists” use computers and technology for hi-tech campaigning and social change. They believe that defacing websites and hacking servers is acceptable as long as it promotes their goals. Regardless of their motives, hacking remains illegal and they are subject to the same computer crime laws as any other criminal.

Overview of U.S. Federal Laws

Although some hackers might have the benefit of bouncing around the globe from system to system, your work will likely occur within the confines of the host nation. The United States and some other countries have instigated strict laws to deal with hackers and hacking. During the past five years, the U.S. federal government has taken an active role in dealing with computer, Internet, privacy, corporate threats, vulnerabilities, and exploits. These are laws you should be aware of and not become entangled in. Hacking is covered under law Title 18: Crimes and Criminal Procedure: Part 1: Crimes: Chapter 47: Fraud and False Statements: Section 1029 and 1030. Each are described here:

Section 1029

Fraud and related activity with access devices. This law gives the U.S. federal government the power to prosecute hackers that knowingly and with intent to defraud, produce, use, or traffic in one or more counterfeit access devices. Access devices can be an application or hardware that is created specifically to generate any type of access credentials, including passwords, credit card numbers, long distance telephone service access codes, PINs, and so on for the purpose of unauthorized access.

Section 1030

Fraud and related activity in connection with computers. The law covers just about any computer or device connected to a network or Internet. It mandates penalties for anyone who accesses a computer in an unauthorized manner or exceeds one’s access rights. This a powerful law because companies can use it to prosecute employees when they use the rights the companies have given them to carry out fraudulent activities.

TIP

Sections 1029 and 1030 are the main statutes that address computer crime in U.S. federal law. Understand its basic coverage and penalties.

The Evolution of Hacking Laws

In 1985, hacking was still in its infancy in England. Because of the lack of hacking laws, some British hackers felt there was no way they could be prosecuted. Triludan the Warrior was one of these individuals. Besides breaking into the British Telecom system, he also broke an admin password for Prestel. Prestel was a dialup service that provided online services, shopping, email, sports, and weather. One user of Prestel was His Royal Highness, Prince Phillip. Triludan broke into the Prince's mailbox along with various other activities, such as leaving the Prestel system admin messages and taunts. Triludan the Warrior was caught on April 10, 1985, and was charged with five counts of forgery, as no hacking laws existed. After several years and a 3.5 million dollar legal battle, Triludan was eventually acquitted. Others were not so lucky because in 1990, Parliament passed The Computer Misuse Act, which made hacking attempts punishable by up to five years in jail. Today, the UK, along with most of the Western world, has extensive laws against hacking.

The federal punishment described in Sections 1029 and 1030 for hacking into computers ranges from a fine or imprisonment for no more than one year. It might also include a fine and imprisonment for no more than twenty years. This wide range of punishment depends on the seriousness of the criminal activity and what damage the hacker has done. Other federal laws that address hacking include:

Electronic Communication Privacy Act

Mandates provisions for access, use, disclosure, interception, and privacy protections of electronic communications. The law encompasses USC Sections 2510 and 2701. According to the U.S. Code, electronic communications "means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic, or photo optical system that affects interstate or foreign commerce." This law makes it illegal for individuals to capture communication in transit or in storage. Although these laws were originally developed to secure voice communications, it now covers email and electronic communication.

Computer Fraud and Abuse Act of 1984

The Computer Fraud and Abuse Act (CFAA) of 1984 protects certain types of information that the government maintains as sensitive. The Act defines the term "classified computer," and imposes punishment for unauthorized or misused access into one of these protected computers or systems. The Act also mandates fines and jail time for those who commit specific computer - related actions, such as trafficking

in passwords or extortion by threatening a computer. In 1992, Congress amended the CFAA to include malicious code, which was not included in the original Act.

The Cyber Security Enhancement Act of 2002 - This Act mandates that hackers who carry out certain computer crimes might now get life sentences in jail if the crime could result in another's bodily harm or possible death. This means that if hackers disrupt a 911 system, they could spend the rest of their days in jail.

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 - Originally passed because of the World Trade Center attack on September 11, 2001. Strengthens computer crime laws and has been the subject of some controversy. This Act gives the U.S. government extreme latitude in pursuing criminals. The Act permits the U.S. government to monitor hackers without a warrant and perform sneak and peek searches.

The Federal Information Security Management Act (FISMA) - Signed into law in 2002 as part of the E-Government Act of 2002, replacing the Government Information Security Reform Act (GISRA). FISMA was enacted to address the information security requirements for non-national security government agencies. FISMA provides a statutory framework for securing government owned and operated IT infrastructures and assets.

Federal Sentencing Guidelines of 1991 - Provide guidelines to judges so that sentences would be handed down in a more uniform manner.

Economic Espionage Act of 1996 - Defines strict penalties for those accused of espionage.

U.S. Child Pornography Prevention Act of 1996 - Enacted to combat and reduce the use of computer technology to produce and distribute pornography.

U.S. Health Insurance Portability and Accountability Act (HIPPA) - Established privacy and security regulations for the health care industry.

Summary

This lesson proves that security is based on the CIA triad. This triad considers confidentiality, integrity, and availability. The application of the principles of the CIA triad must be applied to Information Technology (IT) networks and their data. The data must be protected in storage and in transit.

Because the organization cannot provide complete protection for all of its assets, a system must be developed to rank risk and vulnerabilities. Organizations must seek to identify high risk and high impact events for protective mechanisms. Part of the job of an ethical hacker is to identify potential vulnerabilities to these critical assets and test systems to see whether they are vulnerable to exploits.

The activities described are security tests. Ethical hackers can perform security tests from an unknown perspective, blackbox testing, or with all documentation and knowledge, whitebox testing. The type of approach to testing that is taken will depend on the time, funds, and objective of the security test. Organizations can have many aspects of their protective systems tested, such as physical security, phone systems, wireless access, insider access, or external hacking. To perform these tests, ethical hackers need a variety of skills. They must be adept in the technical aspects of network but also understand policy and procedure. No single ethical hacker will understand all operating systems, networking protocols, or application software, but that's okay, as security tests are performed by teams of individuals where each brings a unique skill to the table.

So, even though "God-like" knowledge isn't required, an ethical hacker does need to understand laws pertaining to hackers and hacking. He must also understand that the most important part of the pre-test activities is to obtain written authorization. No test should be performed without the written permission of the network or service. Following this simple rule will help you stay focused on the legitimate test objectives and help protect you from any activities or actions that might be seen as unethical.

Source: http://www.go4expert.com/articles/ethical-hacking-basics-class-part-1-t11925/