Global Information Assurance Certification Paper

Marian Magel
SANS Security Essentials GSEC Practical Assignment - Version 1.2f

A Journeyman's View of Ethical Hacking

Introduction

What's in a name? Call them hackers, crackers, intruders, or attackers, they are all interlopers who are trying to break into your networks and systems. Some do it for fun, some do it for profit, or some simply do it to disrupt your operations and perhaps gain some recognition. Though they all have one thing in common; they are trying to uncover a weakness in your system in order to exploit it.

The term "hacker" was originally associated with computer enthusiasts who had a limitless curiosity for computer systems. The term "cracker" came about to create a distinction between benevolent and malevolent hackers. However, both terms now represent unauthorized activity that is intended to inflict damage. While early hacking activity was primarily focused on exploring and intellectual challenge, evidence shows that hackers are increasingly turning their attention to financial gain. Case lists of computer and intellectual property crimes can be found on the government's cyber crime web site (http://www.cybercrime.gov/cccases.html).

E-commerce and the need for global inter-connectivity have spurred most companies to do business across the Internet, and connect to outside sources (e.g. customers, partners, and suppliers). As the number of computers on the Internet increase, there will be increased difficulty in keeping them secure. Toolkits exist which enable "hackers" to locate network and system vulnerabilities. Additionally, there are hundreds of informational sites providing "hacking" knowledge. In fact, Macmillan India Ltd. has just published a book by Ankit Fadia, a 16 year old author, entitled The Unofficial Guide to Ethical Hacking. Of course, these resources can also be used to benefit the security professionals as well, but today, attackers have a greater advantage in succeeding at breaching your system than they did ten years ago.

With the advent of the home PC, members of the public now have the opportunity to gain access to significant computing power and sophisticated hardware and software. Hacking techniques that were once practiced by an "elite" group of technically proficient individuals have now become available to anyone with access to the Internet. Further new computer and network technology is becoming more "user friendly," however, architecture intricacies are complicating the way this technology is secured.

As a security professional, you are ever vigilant in your pursuit to avoid and defend against intruder attacks. Ideally, you have a security policy that addresses how intrusions are handled, you have hardened your systems, you have kept OS patches up-to-date, you have installed Firewalls, you employ some type of IDS, and you have instituted a security awareness campaign within your organization. Yeah, right! But at least you are trying. However, are you fighting an up-hill battle since "hacker" activity is continually on the rise? Incident statistics published on the CERT/CC web (http://www.cert.org/stats/) indicate that incidents in 2001 may increase by as much 30% or more over those that occurred in 2000.

Without a way to objectively analyze the risk exposure faced by an organization, these pressures

could lead to reactions causing a desire to over protect your networks and systems, making them difficult to use. As a way to identify threats and countermeasures for these, you may want to consider ethically hacking into your networks and systems in order to identify and address vulnerabilities.

What is Ethical Hacking?

As noted in the article by Sandyha SM, "**Ethical hacking: The network sentinels**" (http://www.ciol.com/content/search/showarticle.asp?artid=21795), "Ethical hacking is a process of simulating an attack by a hacker but without interrupting the systems' function." Ethical hacking sounds like a contradiction in terms, because in our view "hackers" are not ethical. However, performing this type of "testing" to assess technology, provides an organization with the opportunity to enhance its level of computer system controls, through awareness of vulnerabilities.

Vulnerabilities may not be limited to just networks and computer systems, but could include policies that are or more likely are not in place, processes involved with intrusion detection and response, and incident handling procedures including the segregation of duties during an incident. For these reasons, before you begin it is critical to understand what you hope to get out of this type of testing, what the scope of the tests should include, and what inherent risks come with doing an authorized ethical hack.

Benefits of Ethical Hacking

This type of "test" can provide convincing evidence of real system or network level threat exposures through proof of access. Even though these findings may be somewhat negative, by identifying any exposure you can be proactive in improving the overall security of your systems.

However, information security should not be strictly limited to the mechanics of hardening networks and computer systems. A mature security information program is a combination of policies, procedures, technical system and network standards, configuration settings, monitoring, and auditing practices. Business systems, which have resisted simple, direct attacks at the operating system or network level, may succumb to attacks that exploit a series of procedural, policy, or people weak points.

An ethical hack, which tests beyond operating system and network vulnerabilities, provides a broader view of an organization's security. The results should provide a clear picture of how well your detection processes works as well as the response mechanisms that should be in place. "Tests" of this sort could also identify weakness such as the fact that many systems security administrators may not be as aware of hacking techniques as are the hackers they are trying to protect against. These findings could help promote a need for better communication between system administrators and technical support staff, or identify training needs.

Quite often, security awareness among senior management is seriously lacking. Traditional diagnostic work primarily deals with the possibility of a threat and this often leads to a casual view of the threat, deferring the need to immediately address the requirements. Through an ethical hacking exercise, especially if the results are negative, senior management will have a greater understanding of the problems and be better able to prioritize the requirements. For

example, should your ethical hack prove that your firewalls could withstand an attack because there was no breach, but no one noticed the attacks, you may be better prepared to make a case for improving intrusion detection.

Limitations of Ethical Hacking

Ethical hacking is based on the simple principle of finding the security vulnerabilities in systems and networks before the hackers do, by using so-called "hacker" techniques to gain this knowledge. Unfortunately, the common definitions of such testing usually stops at the operating systems, security settings, and "bugs" level. Limiting the exercise to the technical level by performing a series of purely technical tests, an ethical hacking exercise is no better than a limited "diagnostic" of a system's security.

Time is also a critical factor in this type of testing. Hackers have vast amounts of time and patience when finding system vulnerabilities. Most likely you will be engaging a "trusted third party" to perform these test for you, so to you time is money. Another consideration in this is that in using a "third party" to conduct you tests, you will be providing "inside information" in order to speed the process and save time. The opportunity for discovery may be limited since the testers may only work by applying the information they have been given.

A further limitation of this type of test is that it usually focuses on external rather than internal areas, therefore, you may only get to see half of the equation. If it is not possible to examine a system internally, how can it be established that a system is "safe from attack", based purely upon external tests?

Fundamentally this type of testing alone can never provide absolute assurances of security. Consequently, such assessment techniques may seem, at first, to be fundamentally flawed and have limited value, because all vulnerabilities may not be uncovered.

Legal Issues Relating To Ethical Hacking

There are numerous legal issues surrounding ethical hacking, many of which are common sense. For instance, it is illegal to tamper with or otherwise alter physically or logically, equipment belonging to Public Telephone and Telecommunications companies.

The Computer Fraud and Abuse Act, 18 USC Section 1030, prohibits actions most hackers take. "While the development and possession of harmful computer code is not a criminal act, using the code can be." (http://www.pbs.org/wgbh/pages/frontline/shows/hackers/blame/crimelaws.html)

The events of September 11th have helped accelerate changes to cybercrime laws and the desire to adopt these laws. Fifteen EU member states are currently working to create consistent definitions and penalties for computer crimes covering unauthorized access, denial of service, and destruction caused from viruses and worms (http://www.newsbytes.com/news/01/172314.html).

It is critical to ensure the legality of all activities and work prior to beginning an ethical hacking project. Additionally, within some jurisdictions the tests you may be considering could be viewed as illegal, therefore, you will want to have authorization from your organization in writing prior to conducting the exercise. This written permission will provide you with the necessary "get out of jail free card" in the event that you need it.

Opinion from legal counsel may be advisable on some projects before the detailed work plans can be finalized. Further, it is important to ensure that the engagement contract complies with all other commercial legal requirements such as any contractual conditions with any third parties that are to participate in the project.

Objectives Ethical of Hacking

Ethically hacking into your systems should serve to provide your organization with a clear picture of the risk to its technology. It should also help to determine the levels of risk to the business, in order to facilitate intelligent risk management decisions. It should not be meant to promote fear of vulnerabilities, but rather used to for identification and remediation. Therefore, the objectives of this type of testing should include:

- The realistic assessment of business system threats
- The development of threat scenarios which relate the impact of technical vulnerabilities to business risks
- Timely use of the security assessment to apply security solutions

If an ethical hack is performed without factoring in business objectives, there may be an even greater risk that the security assessment, and the remediation strategy, may be unbalanced, being either too rigorous or too permissive. Security assessment, strategy and design must balance these risks

Ethical hacking quantifies and demonstrates risk rather than providing guarantees regarding the adequacy of controls. However, it can help determine:

- How vulnerable an organization is to the latest hacking threats
- How changes in technology can affect the real risk profile of business systems
- How well the organization's security policy has been enforced
- Whether security procedures are being followed
- Where communication or training needs improvement

While these tests may not prove absolute in providing security assurances, they can provide measurement of the level and strength of the security implemented. It should provide a clear picture of an organization's security policy, its ability to identify and respond to attacks, and the security awareness of its management and staff.

Ethical Hacking Project Management Considerations

When conducting an ethical hacking exercise, it is imperative that a number of significant project management principles be addressed before beginning the engagement.

- Scope of the project must be fully defined. A clear definition of the requirements of the project and the objectives of the tests must be documented and agreed to.
- Vendor selection is another critical component to the project since you will be providing confidential information to a "third party." Unless the provider is reputable and trustworthy you may be handing over the "keys to your kingdom."
- The selection of staff for the test team is another critical project item. Staff should be

selected on the basis of their skills, experience, and training. This may be a fine point in negotiating the engagement with your vendor.

- Roles and responsibilities need to be clearly defined at project start-up.
- Engagement contract should provide the necessary authorization for the team to conduct the tests outlined, as well as address any areas that could come into dispute at a later date (i.e. project delays caused by ineffective team)
- The project needs to have appropriate senior level management backing.
- There needs to be formal checkpoints for each phase of the project and as the work progresses.
- A full list of deliverables needs to be established, together with project milestones and dates of delivery.
- Due care must be taken at all times that confidentiality for all aspects of the engagement are complied with.
- Finally, for the project to be successful, information regarding the test periods and testing activities needs to be limited in order to get true test results.

Conclusion

No amount of security monitoring can remove the need for decision making once an intruder is detected. If events are not escalated through management in a timely and appropriate manner, there can be an increased exposure to further unauthorized access or system damage. Procedures must be in place to determine what actions need to be taken in the event of a major intrusion. Appropriate management authorization must be given to all such actions and personnel which may affect the service.

To fully achieve its value to the organization, an ethical hack should test the security mechanisms protecting a system or systems against a particular threat or series of threats. While gaining access to a number of non-specific systems is, in itself, a useful security exercise, it may show nothing about the risk exposures for key systems or practices. By employing a well planned, structured approach, the conclusions you draw from the findings should help towards the implementation of appropriate and cost-effective security solutions.

Therefore, ethical hacking testing should include:

- Testing realistic threats to business by performing realistic threat scenarios
- Analyzing the effectiveness of tested security mechanisms, policies, standards, and procedures
- Identifying weaknesses in existing physical, network, platform and application security
- Testing the co-dependencies and interrelationship of security mechanisms to identify systemic weaknesses
- Testing security event detection, handling, escalation, management and response capability

- Analyzing the findings to determine patterns of weakness and common root causes for these weaknesses
- Raising awareness about potential security weaknesses
- Testing the potential "visibility" of the organization to hackers

References

Bernstein, Terry; Bhimani, Anish B.; Schultz, Eugene; Siegel, Carol A., **Internet Security for Business**, Wiley Computer Publishing, NY, 1996, p 34-38, p 211-212

Skoudis, E., **Counter Hack**, Prentice Hall PTR, NJ, 2002, p 1 – 17

McClure, S., Scambray, J., Kurtz, G., **Hacking Exposed: Network Security Secrets and Solutions**, McGraw Hill, CA,1999, p 3 - 28

CERT/CC Statistics 1988-2001
URL: http://www.cert.org/stats/ (November 2001)

Computer Crime andIntellectual Property Section (CCIPS)
URL: http://www.cybercrime.gov/cccases.html (November 2001)

Palmer, C.C. "**Ethical Hacking**"
URL: http://www.research.ibm.com/journal/sj/403/palmer.pdf (November 2001)

Janet-Cert, **"Penetration Testing"**
URL: http://www.ja.net/cert/JANET-CERT/prevention/pentest.html (November 2001)

Sandyha, S.M. **"Ethical hacking: The network sentinels",** CIOL.com, March 2, 2001
URL: http://www.ciol.com/content/search/showarticle.asp?artid=21795 (November 2001)

Norfork, David, "**Understanding Ethical Hacking"**,PC Network Advisor, March 2001
URL: http://www.itp-journals.com/nasample/M04133.PDF (November 2001)

McAuliffe, Wendy, **"Schoolboy's book on ethical hacking and online hit"**, ZDNet UK, August 7, 2001
URL: http://news.zdnet.co.uk/story/0,,t269-s2092686,00.html (November 2001)

Goldstein, E., Palmer, C., **"Two Views of Hacking",** CNN In-Depth Reports,
URL: http://www.cnn.com/TECH/specials/hackers/qandas/ (November 2001)

U.S. Code: Title 18, Section 1030, Fraud and related activity in connection with computers, as of 01/02/01
URL: http://www4.law.cornell.edu/uscode/18/1030.html (November 2001)

Associated Press, "**FBI: Use racketeering laws against hackers**", USA Today Tech Report, 06/07/00
URL: http://www.usatoday.com/life/cyber/tech/cth376.htm (November 2001

PBS Frontline, "**Computer Crime Laws**", copyright © 2001 PBS On-Line
URL: http://www.pbs.org/wgbh/pages/frontline/shows/hackers/blame/crimelaws.html (November 2001)

McCullagh, D., "**Anti-Terror Bill Not Done** Yet", Wired News, 9/29/01
URL: http://www.wired.com/news/politics/0,1283,47199,00.html (November 2001)

Krebs, B., "**EU Moves to Ratify Cybercrime Terms, Penalties**", Newsbytes, 11/20/01
URL: http://www.newsbytes.com/news/01/172314.html (November 2001)

Last Updated: July 25th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event