Assessing the Information Security Risk Using The Ethical Hacker

GSEC

Practical
Assignment
14 April 2005

Version 1.4c

Option 1

Shannon McDermott
T1 Sydney Australia
20 – 26 Feb 2005

Table of Contents

List of Figures

Abstract

This paper is to be a non-technical guide to ethical hacking. It covers the need for ethical hacking, as well as the methodology utilising reader friendly terminologies and graphics to give any new comer to ethical hacking a good basis and direction for further understanding on the topic.

"Adequately protecting an organisation's assets is a business imperative – one that requires a comprehensive, structured approach to provide protection commensurate with the risks an organisation might face." (ITAC, 2004)

Terms and Definitions

Blue team: The friendly team in opposing forces.
Ethical: Being in accordance with the accepted principles of right and wrong that govern the conduct of a profession.
Expected results: The findings from a specific module
Hacker: A malicious meddler who tries to discover information by poking around.
Intrusion Detection System: A tools designed to monitor and sometimes stop attacks in action, may be host or network based, passive or active.
Liability: The financial assurance of diligence and responsibility. A technical term in law.
Network Scope: This refers to what a tester may legally test.
Non Disclosure Agreement: A legal contract to stop the spread of information beyond the need to know basis of those sharing the NDA.
Pen test: A security test with a defined goal which ends when the goal is achieved or time runs out.
Process: A series of actions, changes, or functions bringing about a result.
Red team: The enemy in opposing forces.
Risk analysis: The process of identifying security risks, determining their magnitude, and identifying areas needing safeguards. .
Silver Bullet: A methodology, practice, or prescription that promises miraculous results if followed - e.g., structured programming will rid you of all bugs
Social engineering: An active attack against processes
Threat: The means through which the ability or intent of a threat agent to adversely affect an automated system, facility, or operation can be manifest.
Vulnerability: A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.
White team: The adjudicators for opposing forces.

Executive Summary

Nearly a third (30%) of respondents in organizations experiencing e-crimes or intrusions in 2003 did not know whether insiders or outsiders were the cause. Respondents who do know report that an average of 71% of attacks come from outsiders compared to 29% from insiders. Regarding the source of the greatest cyber security threat, 40% cited have been hackers, followed closely by current or former employees or contractors (31%). When it comes to identifying specific types of e-crimes committed against organizations, the survey shows 36% of respondents organizations experienced unauthorised access to information, systems or networks by an insider compared to 27% committed by outsiders. Insiders and outsiders for organisations responding to the survey Carnegie –mellon software engineering institute, 2004 commit both sabotage and extortion equally. (Carnegie –mellon software engineering institute, 2004)

The continual growth of hackers as the greatest cyber security threat has created a specialist skill set which is "ethical hacking." The words from Sun Tzu the Art of War- "know your enemy" (Cleary, 1988) could not better describe the ethos of the ethical hacker whose intent is to improve the security of an organisation by becoming the enemy himself. Through this transformation, the ethical hacker can evaluate the effectiveness of the information security process. This enables him to strengthen the security posture, in the eventuality of any further attacks against the organisations information systems.

We have determined that the ethical hacker is on the good side and is of benefit to the organisation. However, organisations need to be aware that there is an element of risk when employing 'ethical hackers', being that there are those who charade as ethical hackers, when they are in fact genuine, criminal hackers with no solid credentials.

We will now explore the processes available by which the ethical hacker can achieve the goal of strengthening organisational security. The first point that needs covered before the ethical hacker can commence any testing is to determine the rules of engagement (ROE). ROE are a set of guidelines that will govern the inherent limitations of a test, these include:

- Time
- Money
- Determination
- Legal restrictions
    a. A solid contract and document outlining the scope of your work often referred to as a 'Get out of jail free card'. This is an authorised document carried by personnel involved in ethical hacking notifying other relevant parties involved, that management are aware of their activities.
    b. Non Disclosure Agreements

c. Liability Insurance, at any stage of testing there is the potential for loss of critical assets, software or information that could be related to a monetary value. Is the tester insured?

- Ethics
- Imposed limitations e.g. only testing Windows systems, permitting the scanning of only certain ports, not including certain critical operational assets.
- Risk analysis

Risk = Vulnerability x Threat

1. What could happen?
2. If it happened, how bad could it be?
3. How often could it happen?
4. How reliable are the answers to the previous questions?

(SANS Institute, 2004)

Once a firm ROE has been established the playing field is set and the ethical hacking can commence.

The work carried out by an ethical hacker can cross many different security areas. The ethical hacker therefore may hold skill sets in any combination of the following categories...

Ethics and Legal Issues
Foot printing
Scanning
Enumeration
System Hacking
Trojans and Backdoors
Sniffers
Denial of Service
Social Engineering
Session Hijacking
Hacking Web Servers
Web Application Vulnerabilities
Web Based Password Cracking Techniques
SQL Injection
Hacking Wireless Networks
Virus and Worms
Hacking Novell
Hacking Linux
IDS, Firewalls and Honey pots
Buffer Overflows
Cryptography
Penetration Testing Methodologies

These skill sets may be shared across a group of individuals, collectively forming an ethical hacking team (E-council, 2005).

The four areas of ethical hacking this paper will examine are*:*

1. Vulnerability assessments
2. Penetration testing

3.Red teaming
4.System tests

Vulnerability Assessments

Vulnerability assessment does just as it states, assesses the security posture of a network for any vulnerability. Once flagged, documented vulnerabilities are compiled for the reporting stage in which all assessment outcomes are briefed to the security administrators. It is important to reiterate that during the vulnerability assessment, the vulnerabilities are highlighted, but not exploited.

Vulnerability assessments are a cost-effective task to carry out, due to the amount of automated tools that are readily available. The tools essentially run checks against a network looking for known vulnerabilities in communications services, ports, routers and operating systems. (Vulnerability lists come compiled by the vendors for their specific product.)

A few well-known vulnerability assessment tools that are readily available are;

ISS Internet Scanner*:* This is a good application internet scanner, but is an expensive option. Organisations need to consider the cost Vs threat when considering the purchase of this tool. Nessus is often used as an effective, more cost efficient alternative.

Nessus: A leading assessment tool, that is readily available. It is a remote security scanner available to suit most common operating systems. This tool is user friendly and has the ability to generate reports and suggest solutions. *(Fyodor)*

Therefore, it is imperative to remember there is no one stop (silver bullet) solution when it comes to security assessments, it is a combination of effective tools good planning and hard work. *"There is no single tool that will find all the system vulnerabilities and characteristics" (Wales, 2003).*

Penetration Testing

Penetration testing is the next step. After completing a vulnerability assessment, the identified vulnerabilities may now be exploited. It is for this exact reason that most IT security groups closely associate vulnerability assessments and penetration testing.

Penetration testing is a way for skilled personnel to take vulnerabilities and exploit them with the final aim of controlling an entire network.

The primary goal of penetration testing is to own the network. The secondary goal is to own the network in as many different ways as possible with the intent of highlighting the system flaws to the administrators and effectively gauging an organisations security posture.

It is important to note that many of the tools utilised in the vulnerability assessment are still of great importance in the penetration test. However, in penetration testing the ethical hacker is going beyond the point of the vulnerability, to the exploitation stage, with the aim of testing the security posture to the limits of the ROE. For example, an ethical hacker may find a vulnerability that allows him to take over 10 out of 20 systems on the network, but if their job is to concentrate on five network systems then this is what they must achieve. The ethical hackers must remain focused on the organisations goals and not become side tracked on personal objectives.

The three stages, which the penetration test can be broken into are;

1. **Discovery:** The discovery of vulnerabilities on any system.
2. **Vulnerability Enumeration**: Matching services to ports, then to known vulnerabilities.
3. **Exploitation:** Proving the list of found vulnerabilities.

(Harris et al, 2004)

Some tools used for penetration testing include:

- Dsniff: This is a series of powerful network auditing and penetration testing tools. This tool has three prominent functions, which include:

    1. The ability to monitor in a passive mode and to inspect network traffic for passwords, files, e-mails etc.
    2. Intercepting and inspecting traffic that is normally unavailable to hackers by utilising layer 2 switching.
    3. Implementing man in the middle attacks by exploiting weak bindings in PKI.

- HPING2 or PING on ‘steroids’ has evolved from ping. It allows for the use of custom ICMP\UDP\TCP packets to be sent and is extremely useful when probing hosts behind firewalls that block standard ping attempts. (Fyodor)

Red Teaming

Red teaming is another component to evaluate the overall security of any given network/system but it differs from penetration testing because*, “penetration testing tests implementation, while red teaming tests design.”* (Peak, 2003).

The terminology red teaming derives from the military term, red team, which describes the enemy in a given scenario. In addition to the red team is the blue team, friendlies and the white team, neutral/judicators. The red team can consist of internal members of the organisation or an external party hired for the task. The blue team can be purposely left unaware of the existence of the red team as a further means of testing their responses, such as Cert Response, IDS Review.

To assess the depth of a security structure you need to understand the likely areas of approach and different types of defences for each area. To help achieve this, the following methods are used:

1*.* Information Security testing

- Document Grinding
- Competitive Intelligence Scouting
- Privacy Review

2*.* Social Engineering

- Request Testing
- Guided Suggestion Testing
- Trusted Persons Testing

3. Internet Technology Security Testing

- Network Surveying
- System Service Identification
- Internet Application Testing
- Routing
- Trusted Systems Testing
- Password Cracking
- Containment Measures Testing
- Denial of Service Testing
- Access Control Testing

4.Communications Security Testing

- PBX Review
- Modem Testing
- Fax Testing

5. Wireless Security Testing

- Wireless Networks Testing
- Cordless Communications Testing
- Infrared Testing
- Privacy Review

6. Physical Security Testing

- Access Controls Testing
- Perimeter Review
- Monitoring Review
- CERT Response Review
- Alarm Response Review
- Location Review
- Environment Review

When these individual areas fit together, they leave a complete security map of any organisation (See figure 1). The security map is useful when examining a single security vector, as it quickly identifies the other security vectors that may used to access the vector under assessment. An example of this is would be when testing the physical security i.e. The location access vulnerabilities of a restricted site. Employing social engineering by gathering information on access points via telephone, e-mail or in person, prior to any physical attempt to access the restricted area.

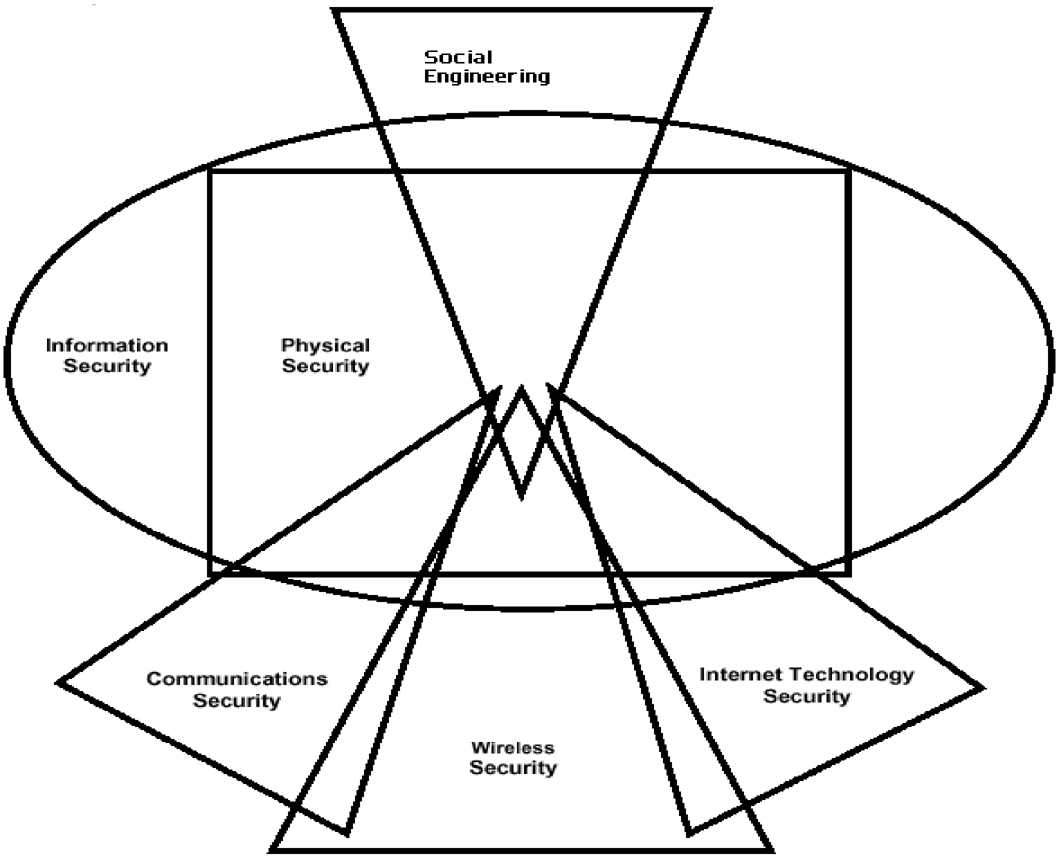

Figure 1. (Herzog, 2003)

The red team conducts tests within the security design to achieve the goals established within the ROE. It is important to mention that the amount of well known and home-grown tools that are available for red teaming are so vast that it is near impossible to cover them all in this paper.

System Testing

A system test is designed to provide a realistic and adequate exposure of the system to all reasonably expected events. (Information Security Policy and Disaster Recovery Associates)

System testing is placing a system i.e. a router, firewall, switch, network device, server, workstation or application, under the microscope and analysing it in every feasible way that the system may interact within its environment. It is only by dissecting a system into its possible attack vectors, then coupling it with further intensive assessing into these vectors, that the knowledge of a system and its vulnerabilities will increase. The two segments of system testing are:

- Foot printing – Gathering as much information as possible on the system in all stages of operations e.g. An application would be assessed to see changes it produces on installation to registry keys (window systems), initialisation files, machine policy, file and directory permission's (Unix) and access control lists,(windows). This would also be the same method of investigation when the system is running in everyday use ports, processes, and registry access) and with the process of uninstallation, checking what remnants of the program are left behind.

- Exploitation – After the completion of footprinting, a thorough list of vectors for exploitation is left. Some vectors that consist of files, registry keys, named pipes, access control lists and network protocol stacks, are the vectors exploited within the ROE of the test.

(Harris et al, 2004)

Due to the nature of system testing and its resemblance to both vulnerability assessing and penetration testing, it allows the use of the previously described tools. The main variation between system testing and vulnerability/penetration testing is that the term 'system' is associated with only one system at any one time, e.g. you can run a vulnerability assessment against an entire network but you can system test one system (router, firewall, switch, network device, server, workstation or application) at a time.

Conclusion

In conclusion it can be seen that ethical hacking, when well planned, is a safe means of testing an organisations IT security. It consists of firstly establishing an ROE that will cover the scope of the ethical hack, followed by vulnerability assessing; to highlight vulnerabilities in the network, penetration testing; the further exploration of the vulnerabilities following the three stages of discover, enumerate and exploit. Red teaming which is the ability to test the overall design of a network and then system test, the systematic dissection of a network system.

Whether ethical hacking is a detriment to the security industry will continue to be a debated issue. However, efforts to coordinate a focal point for ethical hacking and security testing procedures and practices needs to continue. Reference materials such as the Open Source Security Testing Methodology (OSSTM) are an excellent starting point. This and the continual revision and amendment of such documents, in addition to its consistent use by the IT security community, will allow the development of enforceable standards to become a reality. The current security standards allow for a plethora of interpretations/names for what is in essence, the same thing. The lack of standardisation can make a simple task, such as understanding a basic concept and make it a frustrating experience!

In line with having standards for security testing, more time and effort needs to be spent in the legal arena to bring it up to date with today's cyber communities. The current legal loopholes that exist, predominantly arising from the different legislation's between countries, enables the cyber criminal to move freely without ramifications. I believe that international legal standards need integration on a larger scale. This could allow for the punishment and/or extradition of cyber criminals regardless of their country of residence. This would act as a deterrent to aid in the decrease and regulation of cyber criminal activities.

References

Carnegie-Mellon Software Engineering Institute Home Page, 2004. 2004 E-crime watch survey shows significant increase in electronic crimes. Carnegie-Mellon University, PA. 10 Apr 2005.
<http://www.cert.org/about/ecrime.html>

Cleary, T. The Art of War, Sun Tzu. Boston: Shambhala Publications, 1988.

EC- Council Home Page, 2005. CEH, Ethical Hacking and counter measures. International council of E-commerce consultants. 13 Apr 2005.
<http://www.eccouncil.org/EC-Council%20Education/ceh-course-outline.htm>

Fyodor. Home Page. 14 Apr 2005.
<http://www.insecure.org/tools.html>

Harris, Eagle, Harper & Lesten. Grey Hat Hacking: The Ethical Hackers Handbook. McGraw Hill, 2004. 10 Apr 2005.
<http://searchnetworking.techtarget.com/searchNetworking/Downloads/GrayHatHacking_4.pdf>

Herzog, Pete. Open Source Security Testing Methodology Manual. 2003. 14th Apr 2005.
<http://isecom.securenetltd.com/osstmm.en.2.1.pdf>

Information Security Policy and Disaster Recovery Associates Home Page. The Information Security Glossary. 14th Apr 2005.
<http://www.yourwindow.to/information-security/gl_useracceptancetestinguat.htm>

Information Technology Advisory Committee (ITAC). Using ethical hacking technique to asses information security risk, 2003. 8th Apr 2005.
< http://www.cica.ca/itac >

Peak, Chris. Red Teaming: The Art of Ethical Hacking. SANS Practical assignment Version 1.4b (GSEC). July 2003.
< http://www.sans.org/rr/whitepapers/auditing/1272.php >

SANS Institute. Track 1 – Internet security Technologies. Volume 1.3. SANS press, Sept 2004.

Wales, Elspeth. " Vulnerability Assessment Tools". Network Security. July 2003. 14th Apr 2005.
<http://www.compseconline.com/hottopics/hottopic_Nov03/Assessment_tools.p

df>