International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 11
November 2017

A review of Ethical Hacking with its Counter Measures and Cybercrimes

Anamika Srivastava
RRSIMT,amethi

ABSTRACT

One of the fastest growing areas in network security,is ethical hacking. In today's context where the communication techniques have brought the world together; have also brought into being anxiety for the system owners all over the globe. The main reason behind this insecurity is Hacking- more specifically cracking the computer systems. Thus the need of protecting the systems from the nuisance of hacking generated by the hackers is to promote the persons who will punch back the illegal attacks on our computer systems, the Ethical Hackers. It is suggested that cybercrime is becoming organized, large-scale, diversified with increasing division of labor, and is expected to develop increasing ties with offline organized crime. Moreover, offline and online victimization seem to show significant overlap for some crimes. Now that Internet use has become a routine activity in everyday life, criminology as well as criminal law and policy should also incorporate the Internet and cybercrime in their own routine activities, while paying attention to the peculiarities and complexities of the unique phenomenon that is the Internet.

The main purpose of this study is to reveal the brief idea of the ethical hacking and its affairs with the corporate security. This paper encloses the epigrammatic disclosure about the Hacking and as well the detailed role of the ethical hacking as the countermeasure to cracking in accordance with the corporate security as well as the individual refuge. This paper tries to develop the centralized idea of the ethical hacking and all its aspects as a whole. This chapter provides a concise review of literature that has investigated how and why the Internet provides special opportunities to commit crime, and what this implies for the governance of (cyber) crime. It sketches some typologies of cybercrime, and lists twelve risk factors of the Internet that in combination provide a unique opportunity structure for crime. What is known of cybercriminals, organized cybercrime, and cyber victims, and briefly discusses the challenges and limitations of law enforcement and other countermeasure

INTRODUCTION

Understanding the true intentions of the general public is quite a hard task these days, and it is even harder so, to understand the intentions of every single ethical hacker getting into vulnerable systems or networks. Technology is ever growing and we are encountering tools that are beneficial to the general public, but in the wrong hands can create great controversy, breaching our basic right to privacy, respect and freewill. The constant issues highlighted by the media always reporting some type of cyber crime, a study showing that nearly 90% of attacks happen on the inside raising concerns of how easy it is to be working on the inside to be able to infiltrate attacks.

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

Therefore, the term has been broken down into three types:

1. **White hat hacker**—This kind of hacker is often referred to as a security professional or security researcher. Such hackers are employed by an organization and are permitted to attack an organization to find vulnerabilities that an attacker might be able to exploit.

2. **Black hat hacker**—Also known as a *cracker*, this kind of hacker is referred to as a *bad guy*, who uses his or her knowledge for negative purposes. They are often referred to by the media as *hackers*.

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 11
November 2017

3. **Gray hat hacker**—This kind of hacker is an intermediate between a white hat and a black hat hacker. For instance, a gray hat hacker would work as a security professional for an organization and responsibly disclose everything to them; however, he or she might leave a backdoor to access it later and might also sell the confidential information, obtained after the compromise of a company's target server, to competitors. Similarly, we have categories of hackers about whom you might hear oftentimes. Some of them are as follows:

Script kiddie—Also known as *skid*, this kind of hacker is someone who lacks knowledge on how an exploit works and relies upon using exploits that someone else created. A script kiddie may be able to compromise a target but certainly cannot debug or modify an exploit in case it does not work. (From http://cdn.kaskus.com and http://the-gist.org.)

Elite hacker—An elite hacker, also referred to as *l33t* or *1337*, is someone who has deep knowledge on how an exploit works; he or she is able to create exploits, but also modify codes that someone else wrote. He or she is someone with elite skills of hacking.

Hacktivist—Hacktivists are defined as group of hackers that hack into computer systems for a cause or purpose. The purpose may be political gain, freedom of speech, human rights, and so on.

Ethical hacker—An ethical hacker is as a person who is hired and permitted by an organization to attack its systems for the purpose of identifying vulnerabilities, which an attacker might take advantage of. The sole

Important Terminologies Let's now briefly discuss some of the important terminologies that I will be using throughout this book.

Asset An asset is any data, device, or other component of the environment that supports informationrelated activities that should be protected from anyone besides the people that are allowed to view or manipulate the data/information.

Introduction to Hacking □

3 Vulnerability Vulnerability is defined as a flaw or a weakness inside the asset that could be used to gain unauthorized access to it. The successful compromise of a vulnerability may result in data manipulation, privilege elevation, etc.

Threat A threat represents a possible danger to the computer system. It represents something that an organization doesn't want to happen. A successful exploitation of vulnerability is a threat. A threat may be a malicious hacker who is trying to gain unauthorized access to an asset.

Exploit An exploit is something that takes advantage of vulnerability in an asset to cause unintended or unanticipated behavior in a target system, which would allow an attacker to gain access to data or information.

Risk A risk is defined as the impact (damage) resulting from the successful compromise of an asset. For example, an organization running a vulnerable apache tomcat server poses a threat to an organization and the damage/loss that is caused to the asset is defined as a risk.

ARE YOU A HACKER OR CRACKER?

There are hundreds and hundreds definitions of "hackers" on the Web. Combining it all together we get a computer enthusiast, who enjoys learning programming languages and computer systems and can often be considered an expert on the subject, who mastered the art and science of making computers and software do much more than the original designers intended. "Hackers are computer professionals, with skills… Hackers built the Internet. Hackers made the Unix operating system what it is today. Hackers run Usenet. Hackers make the World Wide Web work. If you are part of this culture, if you have contributed to it and other people in it know who you are and call you a hacker, you're hacker" (Raymond E., 2001).A person who breaks into other people's computer systems to get kick out of it or who intent to cause harm is a "cracker". A hacker is a very talented programmer, respected by his peers. True hacker can find plenty of useful projects to work on; breaking things is more a characteristic of children of any age. The basic difference is this: hackers build things; crackers break them. According to Raymond, real hackers consider crackers lazy, irresponsible, and

not very bright and want nothing to do with them. Unfortunately, many journalists and writers have been fooled into using the word "hacker" to describe "crackers", which

is obviously upsets real hackers (Raymond E., 2001).Sadly, we have to join the majority and use the term "hacker" in this paper to refer to individuals who cause so much harm in the society.

Ethical hacking

• Why you need to understand your enemy's tactics

• Recognizing the gray areas in security

• How does this stuff relate to an ethical hacking book?

• The controversy of hacking books and classes

• Where do attackers have most of their fun?

What Is a Penetration Test?

A penetration test is a subclass of ethical hacking; it comprises a set of methods and procedures that aim at testing/protecting an organization's security. The penetration tests prove helpful in finding vulnerabilities in an organization and check whether an attacker will be able to exploit them to gain unauthorized access to an asset.

Vulnerability Assessments versus Penetration Test Oftentimes, a vulnerability assessment is confused with a penetration test; however, these terms have completely different meanings. In a vulnerability assessment, our goal is to figure out all the vulnerabilities in an asset and document them accordingly. In a penetration test, however, we need to simulate as an attacker to see if we are actually able to exploit a vulnerability and document the vulnerabilities that were exploited and the ones that turned out to be false-positive.

Preengagement Before you start doing a penetration test, there is whole lot of things you need to discuss with clients. This is the phase where both the customer and a representative from your company would sit down and discuss about the legal requirements and the "rules of engagement."

Penetration Testing Methodologies In every penetration test, methodology and the reporting are the most important steps. Let's first talk about the methodology. There are several different types of penetration testing methodologies that address how a penetration test should be performed. Some of them are discussed in brief next. The Process and Methodology Planning and Preparation In order to make the penetration test done on an organization a success, a great deal of preparation needs to be done. Ideally a kickoff meeting should be called between the organization and the penetration testers. The kickoff meeting must discuss matter concerning the scope and objective of the penetration test as well as the parties involved. There must be a clear objective for the penetration test to be conducted. An organization that performs a test for no clear reason should not be surprise if the outcome contains no clear result. In most cases the objective of a penetration test is to demonstrate that exploitable vulnerabilities exist within an organization's network infrastructure. The scoping of the penetration test is done by identifying the machines, systems and network, operational requirements and the staff involved. The form in which the results or outcome of the test is presented should also be agreed upon the penetration testers and the organization.

Categories of Penetration Test

When the scope of the penetration test is defined, the category/type of the penetration test engagement is also defined along with it. The entire penetration test can be Black Box, White Box, or Gray Box depending upon what the organization wants to test and how it wants the security paradigm to be tested.

Black Box

A black box penetration test is where little or no information is provided about the specified target. In the case of a network penetration test this means that the target's DMZ, target operating system, server version, etc.,

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 11
November 2017

will not be provided; the only thing that will be provided is the IP ranges that you would test. In the case of a web application penetration test, the source code of the web application will not be provided. This is a very common scenario that you will encounter when performing an external penetration test.

White Box A white box penetration test is where almost all the information about the target is provided. In the case of a network penetration test, information on the application running, the corresponding versions, operating system, etc., are provided. In the case of a web application penetration test the application's source code is provided, enabling us to perform the static/dynamic "source code analysis." This scenario is very common in internal/onsite penetration tests, since organizations are concerned about leakage of information.

Gray Box In a gray box test, some information is provided and some hidden. In the case of a network penetration test, the organization provides the names of the application running behind an IP; however, it doesn't disclose the exact version of the services running. In the case of a web application penetration test, some extra information, such as test accounts, back end server, and databases, is provided.

Types of Penetration Tests There are several types of penetration tests; however, the following are the ones most commonly performed: Network Penetration Test In a network penetration test, you would be testing a network environment for potential security vulnerabilities and threats. This test is divided into two categories: external and internal penetration tests. An external penetration test would involve testing the public IP addresses, whereas in an internal test, you can become part of an internal network and test that network. You may be provided VPN access to the network or would have to physically go to the work environment for the penetration test depending upon the engagement rules that were defined prior to conducting the test. Web Application Penetration Test

Web application penetration test is very common nowadays, since your application hosts critical data such as credit card numbers, usernames, and passwords; therefore this type of penetration test has become more common than the network penetration test.

Mobile Application Penetration Test

The mobile application penetration test is the newest type of penetration test that has become common since almost every organization uses Android- and iOS-based mobile applications to provide services to its customers. Therefore, organizations want to make sure that their mobile applications are secure enough for users to rely on when providing personal information when using such applications.

Social Engineering Penetration Test

A social engineering penetration test can be part of a network penetration test. In a social engineering penetration test the organization may ask you to attack its users. This is where you use speared phishing attacks and browser exploits to trick a user into doing things they did not intend to do.

Physical Penetration Test

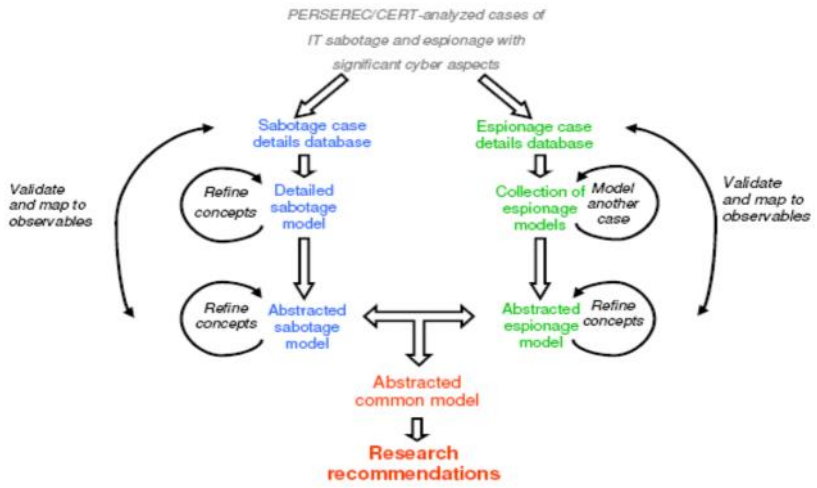
A physical penetration test is what you would rarely be doing in your career as a penetration tester.

In a physical penetration test, you would be asked to walk into the organization's building physically and test physical security controls such as locks and RFID mechanisms.

3. COUNTERING THE PROBLEMS

To counter problems researchers are looking towards new ways of improving ethical hacking and hacking in general from inside the company. One approach is to use models to monitor employees closely to reduce the risk of impact. One solution is to use a model approach that can seriously help in ethical hacking. Not only does this model help; it also tries to reduce the impact by identifying implications early enough to help reduce the impact of confrontation. The model depicted from [9] gives an insight to the problem and how it can be helped. To minimize risks and to further monitor the behavior of ethical hackers and to try to eliminate the problems as and when they occur.

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 11
November 2017



Cyber crimes

The exact prevalence of cybercrime is unknown.

Convictions for cybercrimes are still relatively rare (compared to other crimes), although that does not mean cybercrime is not prevalent (Smith et al., 2004, pp. 25-29). There is supposed to be a high 'dark number' of undetected, unreported, uninvestigated, or unresolved cybercrimes, due to the invisibility and complexity of digital traces and a general reluctance of business victims to report for fear of reputation damage To understand cybercrime, it is useful to make some distinctions, since the motivations and modi operandi of perpetrators may differ for various types of cybercrime. The most common distinction is between the Internet as a tool or as a target.

The criminalizes:

1. offences against the confidentiality, integrity and availability of computer data and systems; these include illegal access (hacking),

The Internet First Part: Risk Factors - Environment 739 illegal interception, data interference (e.g. viruses), system interference (e.g., denial-of-service attacks), and misuse of devices (e.g., possessing hacker software);

2. computer-related offences; these include forgery and fraud;

3. content-related offences and copyright offences; the former covers child pornography (racism is included in a separate Protocol to the Convention).

These features of the Internet form the basis of 12 specific, interrelated, risk fact ors that facilitate cybercrime. The Internet:

1. has a *global reach*, enabling perpetrators to look for the most vulnerable computers and victims anywhere in the world without having to leave home or the next-door Internet café

2. related to this, leads to *deterritorialisation*, which implies that cybercrime is almost by definition international, with consequent legal challenges of jurisdiction and cross-border co-operation;

3. allows for decentralized, *flexible networks* in which perpetrators can (loosely) organize themselves to divide labor or to share skills, knowledge, and tools

4. facilitates *anonymity*, at least for perpetrators who have the knowledge and take some effort of using anonymisation tools such as remailers and torrent networks; however, also less tech-savvy perpetrators are (or feel) relatively anonymous when they operate at a (large) distance from behind an IP number, email address, or scam Facebook profile that is often not easy to trace to a specific individual

5. enables *distant interaction* with victims, removing potential social barriers that perpetrators face in physical, person-to-person interaction; cybercrime thus involves 'anonymous, networked and rhyzomatic relations between perpetrators and victims'

6. facilitates *manipulability* of data and software with minimal cost, because it is based on digital representation (allowing for copying without loss of quality, and altering without visible traces) and because the Internet was built as an open infrastructure with intelligence at the end points to foster innovation by end-users;

7. allows for *automation* of criminal processes, where one piece of software launched on the Internet can replicate and attack millions of computers at the same time – but also over longer periods of time – and where basic software such as a sample virus can be easily customized by so-called 'script kiddies' to create a new virus (Wall, 2007);

8. can blow up the *scale* of a crime from a minor nuisance to major harm, for example when a virus has far graver consequences than a curious script kiddies imagined, or when a remark or (sex) photograph posted online acquires a global and permanent reach; for example, 'harassment writ large in cyberspace – expanded so drastically in target, scope, and reach – has far greater impact than any schoolyard attack'

9. allows for *aggregation* of a large number of insubstantial gains, for example, through salami techniques more in general, cybercrime often has many victims with relatively small damage each; this *de minims* problem may be one of the biggest challenges of cybercrime

The Internet First Part: Risk Factors - Environment 741 since it reduces incentives to report, investigate, and prosecute the crime (Wall, 2007);

10. facilitates an *information economy* where information has become a valuable asset, both in the legal market (e.g., music, movies, software, books) and in the black market, where credit-card numbers, personal information, and passwords are traded to facilitate fraud and theft (Wall, 2007: 32);

11. has structural *limitations to capable guardianship* that can serve as a social or technical obstacle to commit crime

12. has *rapid innovation cycles*, allowing for new techniques and tools to be developed in short periods for

Conclusion and future scope

- From the above discussion we can conclude that no one can fully secure their system until and unless they have proper knowledge of attempts of attack. So there are several method in which way one can hack any system or network. In ethical hacking is the attempts to find weakness in any system and recover it. It is for legal purpose only. while in cybercrime person have intention to harm the system or to stole some information by cracking. Cracking is the attempt in which attacker tries possible attempts to crack the password and stole the information for their personal use.
- There are very scope for research to find the way to secure our network. It can be applicable in the area where to find weaknesses and recover the system. One cane use it for the social purpose not for self. More convenient way it to prevent suspicious person to enter the network. Several polices can be invented to stop the outsider to enter the network. In this way can try to reduce the possibility to be hacked by someone.

REFERENCES

- From http://cdn.kaskus.com and http://the-gist.org.
- Ethical Hacking and Penetration Testing Guide - Baloch, Rafay
- Gray Hat Hacking The Ethical Hackers Handbook, 3rd Edition
- Hacking-and-Cybercrime
- A Model of Unethical Usage of Information Technology
- Ethical_Hacking_The_security_justification_redux