Study of Ethical Hacking and Management of Associated Risks

Mohammed Abdul Bari
Dept. of Computer Science & Engineering
Nawab Shah Alam Khan College
of Engineering & Technology
Hyderabad, India.

Shahanawaj Ahamad
Dept. of Computer Sc. & Software Engineering
College of Computer Sc. & Engineering
University of Hail
Hail, Saudi Arabia.

***Abstract* - Hacking has become an extensive trouble with the beginning of the digital age, almost worldwide access to the internet and other digital media. It is significant for individuals, corporations, and the government to guard them from being susceptible to such attacks. The purpose of this paper is to provide information about ethical hacking; their skill to share advanced security knowledge and capabilities with organization and pointing out their vulnerabilities.**

Keywords—hackers; ethical hacking; risk management; risk assessment; network hacking.

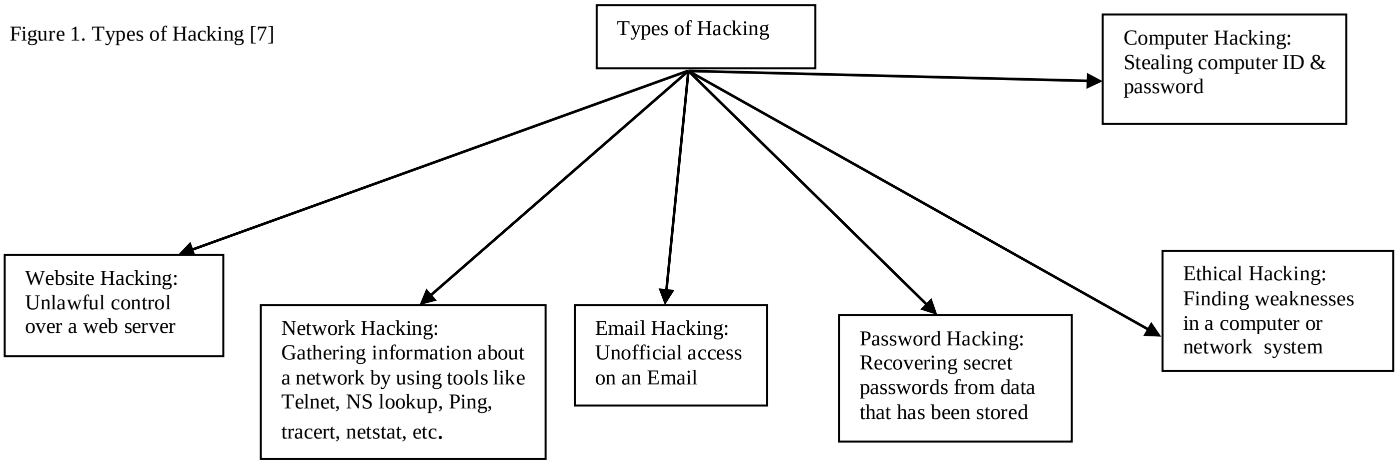
I. Introduction

A hacker is an intelligent professional who likes to mess with software or electronic systems, consequently harms the organizations and individuals IT assets economically and socially if working negatively. They enjoy exploring to educate them self how to hinder, temper computer systems functions. They love discovering new ways to work with computer system [2]. As the esteem of computers and their sustained high cost, a few users would defy the access pedals that had been put in place. They would pinch passwords or account numbers by looking over someone's shoulder, discover the system for bugs that might get them past the rules, or even take cope of the whole system. They would do these things in order to be able to run the programs of their choice, or just to change the confines under which their programs were running. Initially these computer intrusions were fairly benign, with the most damage being the theft of computer time [1]. Sporadically the less endowed, or less careful, intruders would accidentally bring down a system or harm its files, and the system administrators would have to restart it or make maintenance other times, when these intruders were another time denied access once their activities were exposed, they would react with determination destructive actions and when the number of these destructive computer intrusions became noticeable, due to the visibility of the system or the extent of the damage inflicted, it became "news". Instead of using the more precise term of "computer criminal", the media began using the term "hacker" to describe folks who break into computers for fun, revenge, or profit. Since calling someone a "hacker" was initially meant as a tribute, computer security professionals prefer to use the term "cracker" or "intruder" for those hackers who turn to the dark side of hacking [3].

II. Ethical Hacking

With the growth of the Internet, a computer safety measure has become a major anxiety for businesses and governments. They fancy being able to take benefit of the Internet for electronic commerce, publicity, in sequence distribution and admission, and other pursuits, but they are concerned about the prospect of being "hacked". The probable patrons of these services are worried about maintaining control of personal information that varies from credit card numbers to social security numbers and home addresses [1]. In their search for a way to approach the problem, organizations came to understand that one of the best ways to assess the intruder threat to their interests would be to have self-governing computer security professionals attempt to break into their computer systems. This scheme is similar to having self-governing auditors come into an organization to verify its bookkeeping records. In the case of computer security, these "tiger teams" or "ethical hackers" [4] would use the same tools and techniques as the intruders, but they would neither damage the target systems nor steal information. Instead, they would assess the target systems' security and report back to the owners with the vulnerabilities they found and instructions for how to remedy them. This method of evaluating the security of a system has been in use starting the early days of computers. In one early ethical hack, the United States Air Force conducted a "security evaluation" of the Multics operating systems for "potential use as a two-level (secret/top secret) system" [5]. Hacking is usually legal as long as it is being done to find weaknesses in a computer or network system for testing purpose. This sort of hacking is called Ethical Hacking [6].

Figure 1. Types of Hacking [7]


Types of Hacking
Computer Hacking: Stealing computer ID & password
Website Hacking: Unlawful control over a web server
Network Hacking: Gathering information about a network by using tools like Telnet, NS lookup, Ping, tracert, netstat, etc.
Email Hacking: Unofficial access on an Email
Password Hacking: Recovering secret passwords from data that has been stored
Ethical Hacking: Finding weaknesses in a computer or network system

A. Path Taken by Hackers [11,12]:

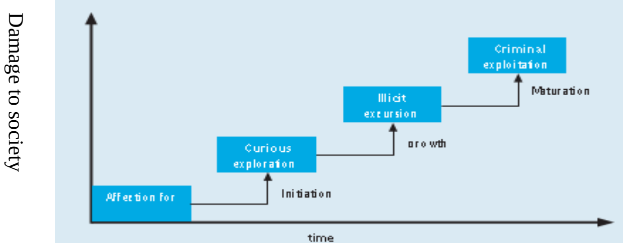


Figure 2. Growth of Hackers [11]

- Initiation: Development in early interest in computers
- Innocent motives: Hear the subjects wanted to know more about computers, and enhance their online experiences, in order to do so it to alter existing software or overcome network restrictions.
- Growth: Hacker preferred to spend their time learning hacking skills. Hackers organized into loosely associated groups and practical or real communities, obtain technical skills through mentoring and sharing, and establish social orders, group norms, and individual and social identities
- Maturation: Associate with other hackers: If I have a problem, I go to the experts for an answer. Asked someone who's already done it. Hackers felt they knew the difference between right and wrong, and have not stepped over the line. The number one enabler is the lack of security and the abundance of software vulnerabilities. One thing that successful hacks have in universal is the aptitude to remain secret – right up until the moment that the time is right and the attackers strike.

B. Path taken by Hackers

This section explained the phases of ethical hacking as shown in fig.3.

- Phase 1: Reconnaissance

This is divided into two phases as Passive reconnaissance and Active reconnaissance. Passive reconnaissance involves congregation information about a possible target lacking the targeted individual's or company's information. Active reconnaissance involves probing the network to discover individual hosts, IP addresses, and services on the network. Both passive and active reconnaissance can lead to the discovery of useful information to use in an attack. Example, it's usually easy to find the type of web server and the operating system version number that a company is using. This information may allow a hacker to find vulnerability in that OS version and exploit the vulnerability to gain more access.

- Phase 2: Scanning

Scanning involves taking the information discovered during reconnaissance and using it to examine the network.

- Phase 3: Gaining Access

Hear where the real hacking takes place. Vulnerabilities which are uncovered during the reconnaissance and scanning phase are now exploited to gain access to the target system. The hacking attack can be delivered to the target system via a local area network (LAN), either wired or wireless

- Phase 4: Maintaining Access

Formerly a hacker has gained access to a target system; they want to keep that access for future exploitation and attacks. They can use it as a base to launch additional attacks. In this case, the owned system is sometimes referred to as a zombie system [4].

- Phase 5: Covering Tracks

Formerly hackers have been able to gain and maintain access; they cover their tracks to avoid detection by security personnel, to continue to use the owned system, to remove evidence of hacking, or to avoid legal action.

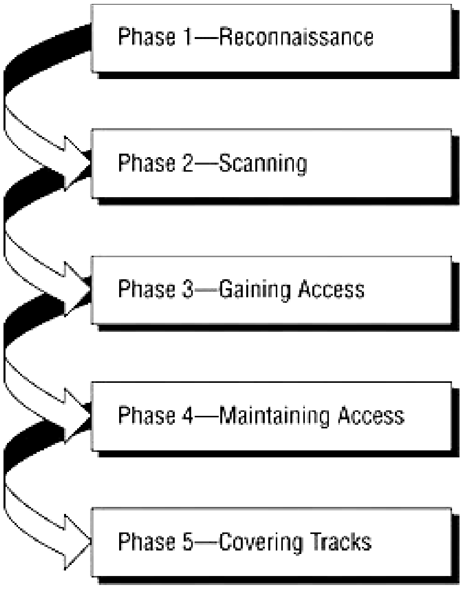


Figure 3. Phases of ethical hacking

C. *Path taken by Hackers Why Ethical Used in Organization*

Ethical hacking companies offer tremendous value in their skills to share their sophisticated security and organizational knowledge and knowledge. This examines enables businesses to adjust their security technologies, train their staff, and ratify security practices that improved protect dangerous systems and responsive data. Ethical hacking services offer organization with purpose and real-world assessments of security weaknesses, vulnerability, risk, and remediation options. As a result, ethical hacking is rapidly gaining attention as an essential security practice that should be performed on a regular basis [6]. They are highly paid professionals with a rightful status. They can reduce the risk of impact, clearly identifying reimbursement and flaws helping senior company directors to appreciate if such tricks should be undertaken. Ethical hackers could explore vulnerabilities earlier to minimize the risk. The company could presume diffusion tests to find if they are susceptible to attack. Finding vulnerabilities for companies not only helps the company but also minimizes the risks of attacks, though ethical hackers have five days in universal to carry out tests, what happens if vulnerabilities are overlooked. If an ethical hacker fails to deliver results to the business and assume the system is safe and that it has no problems, which can be liable for legal actions if a hateful hacker gets into the system [3].

Major organizations such as Google, RSA, and Sony have lately made headlines as sufferers of highly complicated cyber-attacks that appear in major security breaches and data loss. Data security crack can involve massive amounts of sensitive customer data such as credit card numbers, social security numbers, passwords, and PINs. 77 million customer records were leaked in the 2011 Sony Networks data violate. In other cases, security breaches can absorb the loss of precious scholar property or hush-hush state secrets.

III. Vulnerability Assessment Of An Organization By Ethical Hacking

A vulnerability evaluation is a procedure, [8] which is a part of the Vulnerability Management Program, whose idea is to examine a given system for possible points of breakdown and measure their scale after that. Its scope encompasses not only the companies' technological possessions – i.e., systems and networks – but also their physical truthfulness and security measures concerning the safety of personnel. Such a wide perimeter to content determines the variety of techniques designed to perform the vulnerability assessment, namely scanning tools, physical checks, and social engineering tests.

A. *Risk Assessment*

Create a record list of all resources and assets (e.g., networks, systems, personally identifiable information, etc.) Evaluate these company assets and resources and assign them values Catalog the vulnerabilities and define the potential threats to each asset/resource and these can be done by risk analysis [9]. Many factors are measured when performing a risk analysis: asset, vulnerability, threat and impact to the company. An example of this would be an analyst trying to find the risk to the company of a server that is vulnerable to Heartbleed [10]. A risk analysis, when concluded, will have a final risk rating with explanatory controls that can further reduce the risk. Business managers can then take the risk report and mitigating controls and decide whether or not to implement them. To carry out a Risk management, we must first recognize the possible threats that we face, and then estimate the likelihood that these threats will materialize. Risk Analysis can be complex, as you'll need to draw on detailed information such as project plans, financial data, security protocols, marketing forecasts, and other relevant information. However, it's an essential planning tool, and one that could save time, money, and reputations.

The three different concepts explained here are not elite of each other, but somewhat harmonize each other. In many information security programs, vulnerability assessments are the first step – they are used to carry out wide sweeps of a network to find absent patches or misconfigured software. From there, one can either perform a penetration test to see how usable the vulnerability is or a risk analysis to ascertain the cost/benefit of fixing the vulnerability. Of course, you don't need either to perform a risk analysis. Risk can be determined anywhere a threat and an asset is present. It can be data center in a hurricane zone or confidential papers sitting in a wastebasket.

Penetration Testing is a method that many companies follow in order to minimize their hazard in security breaches [6], they are as follows:

- Black Box − In back box, the ethical hacker doesn't have any in sequence about the infrastructure of the organization that he is trying to break in. Here, hacker tries to find the in sequence by his own way.

- White Box − In white-box breach testing, the ethical hacker is provided with all the essential information about the infrastructure and the set of connections of the organization that he needs to break in.
- Grey Box − It is a type of breach testing where the ethical hacker has an incomplete knowledge of the infrastructure, like its domain name server.

TABLE I: TESTING ADVANTAGES AND DISADVANTAGES[6]

	Advantage	**Disadvantages**
Black Box Testing	• Real world result • Less project risk	• Less encompassing • More effort obligation
White Box Testing	• More encompassing analysis • More efficient auditing	• Large Project and more cost • Less real-world data
Grey Box Testing	• Balance of cost/time and assessment scope • Provides analysis not possible with pure black or white box tests	• Need for more careful project planning such as scope and expectations

To carry out a Risk Analysis, you must first identify the possible threats that you face, and then estimate the likelihood that these threats will materialize. Risk Analysis can be multifaceted, as you'll need to draw on detailed information such as project plans, financial data, security protocols, marketing forecasts, and other relevant information. However, it's an essential planning tool, and one that could save time, money, and reputations.

B. Impact on Operations

Ethical hacking consultations can be a very time intense speculation and will necessitate some level of communication with the customers' end-users, administration, IT staff, and security staff. Businesses trepidation that this can be disturbing to the daily operations of the IT staff and end-users which would outcome in lost efficiency [14]. However, the customer should conclude the level of communication that the ethical hackers will begin with personnel during the preparation stage. This communication is a significant variable that customers can strangle to keep costs and distractions to a minimum during a penetration test. Unfortunately, hackers use social engineering methods to trick end-users into divulging information or credentials and thereby allow a security breach. As a result, the ethical hacker may be useful for security assessment and evaluation.

IV. HOW AN ORGANIZATION PROTECT HIMSELF FROM HACKING

- Install a good approved anti-virus on server side as well as sand alone system [13].
- Constantly have your Windows Firewall turned on.
- Never ever trust warez sites. There is a lot of malware flowing out there.
- Don't run .exe programs specified by anyone.
- Disable pen drive option.
- Don't run attachments from emails.
- If you want to run .exe files safely, run them sandboxed. A free application Sandboxie is available for this purpose.

V. CONCLUSION

The thought of testing the security of a system by annoying to break into it is not new. Whether an automobile corporation is crash-testing cars, or an entity is testing his or her skill at martial arts by infighting with a partner, evaluation by testing under attack from a real adversary is widely accepted as prudent. It is, however, not sufficient by itself. Standard auditing, watchful intrusion detection, good system management practice, and computer security awareness are all essential parts of an organization's security efforts. A single failure in any of these areas could very well expose an organization to cyber-vandalism, discomfiture, loss of proceeds or mind share, or worse. Any new technology has its benefits and its risks. While ethical hackers can help clients better understand their security needs, it is up to the clients to keep their guards in place. The threat and risk assessment are the integral part of the overall life cycle of the infrastructure.

REFERENCES

[1] S.Garfinkel,"Database notation" ,O'Reilly & Associates ,Compbridge, MA 2000.

[2] D.Jamil,M.N.Ali.Khan"Is Etghical Hacking Ethical?",IJEST, vol 3 May 2011.

[3] C.C.Plamer,"Ethical hacking ",IBM System Journal,vol 40,No 3,2001.

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

[5] P. A. Karger and R. R. Schell, Multics Security Evaluation: Vulnerability Analysis, ESD-TR-74-193, Vol. II, Headquarters Electronic Systems Division, Hanscom Air Force Base, MA June 1974.

[6] Frost & Sullivan,"The Importance of Ethical Hacking",A Frost & Sullivan White Paper, April 2012.

[7] Tutorialspoint,"Ethical Hacking Overview",Tutorialspoint simple easy learning . https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_overview.htm

[8] Infosec Institute,"Penetration Testing Benefits:Pen Testing for Risk Management ",Info Sec Intitude Resources, October 2016.

[9] Tony Martin-Vegue ,"Cyber Security for Business Leaders",IDG Contributor Network, May 2015. http://www.csoonline.com/article/2921148/network-security/whats-the-difference-between-a-vulnerability-scan-penetration-test-and-a-risk-analysis.html

[10] Codenomicon,"The Heartbleed Bug",online retrieved http://heartbleed.com/

[11] Zhengchuan,Qing Hu,Chenghong Zhang," Start with talent and Skill driven by curiosity and hormones ,constrained only by moral values and judgment ",Communications of ACM, vol 56,no 4,April 2013.

[12] Michael Kassnern," Hacker: From innocent curiosity to illegal activity ",IT Security News latter ,May 2013

http://www.techrepublic.com/blog/it-security/hackers-from-innocent-curiosity-to-illegal-activity/

[13] Mahesh," How do Hackers Hack your Passwork", Block for Blogger ShoutMe,April 2015.

[14] M.A.Bari & Shahanawaj Ahamad ," Process of Reserve Engineering of Enterprise Information System Architecture ",IJCSI,vol 8,Iss 5,no 3,Spetember 2011.