IJASRM

International Journal of Advanced Scientific Research and Management, Volume 4 Issue 12, Dec 2019

www.ijasrm.com

ISSN 2455-6378

Ethical Hacking: The Art of Manipulation

Shehan Shetty[1] and Kshitij Shetty[2]

[1]Department of Computer Engineering, St John College of Engineering and Management, Palghar, Maharashtra -401404, India

[2]Department of Computer Engineering, St John College of Engineering and Management, Palghar, Maharashtra -401404, India

Abstract

Hacking generally refers to an unauthorized intrusion into a computer or a network. The person engaged in hacking activities is known as a hacker. State of security on the internet is very poor, hence private and public organizations promote persons who will retort back the illegal attacks which are possible on their systems. Usually the intent behind unauthorized hacking is to steal valuable data for future use, manipulation or espionage, interruption of an on-going service, or to extort money. Ethical hacking is an activity to find and rectify the vulnerabilities of the system. This paper describes ethical hacking, its types and its impact on businesses and governments.

Keywords: *ethicalhacking, security, hackers, vulnerabilities*

1. Introduction

1.1 Ethical Hacking

Ethical Hacking sometimes called as Penetration Testing is an act of intruding/penetrating into system or networks to find out threats, vulnerabilities in those systems which a malicious attacker may find and exploit causing loss of data, financial loss or other major damages. The purpose of ethical hacking is to improve the security of the network or systems by fixing the vulnerabilities found during testing. Ethical hackers may use the same methods and tools used by the malicious hackers but with the permission of the authorized person for the purpose of improving the security and defending the systems from attacks by malicious users.

The technology of internet of things is growing at rapid rate. Things are getting connected to internet and the only way to secure them is to keep a password. Hackers tend to break through this line of protection, by various means like the brute force method, man in the middle attack and dictionary attack. These days complex password breaking algorithms have been developed, which perform the attacks with a significantly higher efficiency.

Ethical hackers advise firms that hire them to have a better security so as to protect themselves against such upcoming attacks. To make a system secure, the ethical hacker will behave just like an actual hacker and try to exploit the system. Ethical hackers are aware of the various techniques that the criminal hackers employ and they make use of them to find vulnerabilities of the system, in order to fix them.

1.2 Need for Ethical Hacking

1.2.1 Defensive Strategies with Offensive Approach

An employed ethical hacker finds vulnerabilities and weaknesses of your existing entities with the intention of fixing them. This basic definition of ethical hacking depicts how the offensive actions of an ethical hacker are used to build defensive strategies to protect a company’s critical data and entities.

1.2.2 Limits Your Liability

Having an ethical hacker in your organization not only strengthens your data security but it also limits your organization’s liability when under a cyberattack. Hiring a certified ethical hacker to perform the task shows your commitment to the system/network security. With a professional at work, you will face less pushback from your clients and be protected from a compromise of critical data at the time of an attack.

1.2.3 Handle Sophisticated Attacks

With the growing force of the dark web and malicious hackers, present-day cyberattacks are more sophisticated in nature than before. Now, it is difficult to detect the notorious activities of a hacker in the absence of an intelligent intrusion detection system. Well, an ethical hacker can help your organization to define detection rules which can eliminate the chances of various cyberattacks.

1.2.4 Protect the Credibility of Your Organization

It has been noticed in the past that a security breach can harm your credibility in the market. 2015's Facebook data breach resulted in the company's share price dropped nearly 7% on the third day after Facebook confirmed the breach. Even the market value of the company witnessed a decline after the Cambridge Analytica scandal. That's where a certified ethical hacker comes into the picture. With an onboard ethical hacker, you will be less susceptible to such data breaches

1.2.5 Easy Cloud Transition

These days virtualization and IT sourcing are the common trends. But with these trends, the simultaneous transition to the cloud offers numerous ways for malicious hackers to misuse the newly vulnerable entry points. In such a scenario, an ethical hacker can help you to keep your network secure and protected during cloud transition

2. Types of Hackers

Hackers can be classified into different categories such as white hat, black hat, and grey hat, based on their intent of hacking a system. These different terms come from old Spaghetti Westerns, where the bad guy wears a black cowboy hat and the good guy wears a white hat. It is said that lighter the color, the lesser is their intention to harm.

2.1 White Hat Hackers

White Hat Hackers are authorized and paid person by the companies, with good intends and moral standing. They are also known as "IT Technicians". They never intent to harm the system, rather they try to find out the weaknesses in a Computer System as a part of penetration testing.

By 1981, The New York Times described white hat activities as part of a "mischievous but perversely positive hacker tradition". Not all hackers are motivated by greed, but some of them want to use their powers for good.

White Hat hackers can also earn a healthy amount of money working for organizations. There are also independent white hat hackers who find out errors in applications or websites of many organizations. The current record-holder for the highest-value bug bounty is Google's $112,500 payment to a Chinese researcher who discovered a remote exploit vulnerability in Android.

2.2 Black Hat Hackers

Black hat hackers can range from teenage amateurs who spread computer viruses to networks of criminals who steal credit card numbers and other financial information. Black hat hacker activities include planting keystroke-monitoring programs to steal data and launching attacks to disable access to websites. Malicious hackers sometimes employ non-computer methods to obtain data, for example, calling and assuming an identity in order to get a user's password.

Black hat hackers have their own conventions, of which two of the more prominent are DEFCON and Black Hat. Black hat conventions are often attended by security professionals and academics who want to learn from black hat hackers. Law enforcement officials also attend these conventions, sometimes even making use of them to apprehend a black hat hacker, as occurred in 2001 when a Russian programmer was arrested the day after DEFCON for writing software that decrypted an Adobe e-book format.

2.3 Grey Hat Hackers

Grey Hat Hackers are a blend of both white hat and black hat hackers. A Grey Hat Hacker gathers information and enters into a computer system to breech the security, for the purpose of notifying the administrator that there are loopholes in the security and the system can be hacked. They act without malicious intent but just for fun.

Many people see the world of IT security as a black-and-white world. However, gray hat hacking does play a role in the security environment. One of the most common examples given of a gray hat hacker is someone who exploits a security vulnerability in order to spread public awareness that the vulnerability exists. In this case, experts might say that the difference between a white hat hacker and a gray hat hacker is that the gray hat hacker exploits the vulnerability publicly, which allows other black hat hackers to take advantage of it. By contrast, a white hat hacker may do it privately in order to alert the company, without making the results public

3. Steps of Ethical Hacking

There are 5 phases that are generally followed to perform a successful hack. They are:

3.1 Reconnaissance

Reconnaissance is also called footprinting and information gathering. It is the preparatory phase where the hackers collect as much information as possible about the target. Collection of information is usually about network, host and people involved.

3.2 Scanning

Three types of scanning are involved:

a. Port scanning: This phase involves scanning the target for the information like open ports, live systems, and various services running on the host.

b. Vulnerability Scanning: Checking the target for weaknesses or vulnerabilities which can be exploited. Usually done with help of automated tools.

c. Network Mapping: Finding the topology of network, routers, firewalls servers if any, and host information and drawing a network diagram with the available information. This map may serve as a valuable piece of information throughout the hacking process.

All of this serves as a base to develop a strategy to perform the attack. Hence this is an indispensable step in the process of hacking, followed by most of the hackers.

3.3 Gaining Access

This phase is where an attacker breaks into the system/network using various tools or methods. After entering into a system, he has to increase his privilege to administrator level so he can install an application he needs or modify data or hide data.

3.4 Maintaining Access

Hacker may just hack the system to show it was vulnerable or he can be so mischievous that he wants to maintain or persist the connection in the background without the knowledge of the user. This can be done using Trojans, Rootkits or other malicious files. The aim is to maintain the access to the target until he finishes the tasks he planned to accomplish in that target.

3.5 Clearing Track

A criminal hacker will always clear all evidence so that in the later point of time, no one will find any traces leading to him. This involves modifying/corrupting/deleting the values of Logs, modifying registry values and uninstalling all applications he used and deleting all folders he created.

4. Impact of Ethical Hacking

Ethical Hackers systematically attempt to penetrate a computer system or network on behalf of its owners. Their sole purpose is to find security vulnerabilities that a malicious hacker could potentially exploit. In the past companies used to rely on the basic built-in security of the system, to prevent attacks. But this approach is no longer effective and sensible. The skills of the attackers as well as the variety of tools in their arsenal make a static security system obsolete. The system must steadily keep getting better with the help of a helpful White Hat hacker in order to weather the new and innovative attacks.

Ethical Hacking to strengthen system security has become one of the most essential parts of software development life cycle. Cyber Laws strongly recommend inclusion of a cyber security team, with a White Hat Hacker in it, in a Software Development Team, when the said software would be dealing with public data.

The practice of Ethical Hacking has allowed the evolution of security systems at an unprecedented rate. But if the allegiance of the employed ethical hacker is compromised, then the company in question stands to lose a lot. This is an issue, along with the presumable incompetence of the hired hacker that companies must always be mindful about. The sense of never truly being safe is prevalent, with respect to their cyber properties and rights.

Courses to learn ethical hacking, quite often end up being misused. This is an unfortunate effect of the wide-spread propagation of ethical hacking, and one of the major sources of new black hat hackers. This is difficult to regulate and have a hold over, and one of the only ways to reduce damage due to this, is by minimizing the contents of such freely available courses to a basic level.

As the system security steadily improves, the attackers themselves improve their attacking techniques, by coming up with new and innovative attack strategies. They continuously persevere to find new vulnerabilities in the system’s security. This makes the job of ethical hackers a perpetual cycle of system protection from the endlessly developing attacks.

According to surveys conducted by cyber security firms in the country, Indian firms lost more than $4 billion in 2013 alone because of hackers. With more and more companies entering the e-commerce ecosystem and adopting new technologies like cloud computing, the threat from imminent security breaches is clearly demanding the need for efficient information security systems. The rising threat from cyber-attacks has exposed the severe shortage of talent in this sector.

The demand for ethical hackers is at an all-time high. According to NASSCOM, 59% of organizations have vacant cybersecurity positions suggesting a shortfall of 1.5 million by 2020 globally. As per 2015 figures reported by NASSCOM, India needed more than 77,000 white hat hackers as against only a mere 15,000 certified professional ethical hackers in that year. This figures increases at an alarming rate with each year. This huge demand, in turn, has led to a sharp increase in the pay package of professionals who can fit the cybersecurity roles. Professionals are being paid anything from double their IT salaries to 10 times the average salary of an IT engineer to fill up this gap.

5. Conclusions

Ethical Hacking is an indispensable part of the current technological ecosystem. It may have a few regrettable disadvantages, but the overall benefits outshine them. The absence of an ethical hacking infrastructure in a company may be highly detrimental, especially with the growing concerns for safety of intellectual property.

Ethical hacking plays a vital role in maintaining and saving information. It all depends on the intention of hacker. It is almost impossible to fill a gap between an ethical and a malicious hack as human mind cannot be conquered, but security measures can be tightened.

It can be concluded that ethical hacking is one of the positive aspects of networking that strengthens and reinforces cyber security.

Acknowledgments

We would like to express our deepest appreciation to all those who provided us with the resources and assisted us in completing this paper. We would like to start by offering our heartfelt gratitude to our teacher, Mr. Chetan Patil, who was always forthcoming with his desire to teach. It was one of the most important factors that generated an interest within us, for this field. Next, we thank our parents and all of our friends, who provided us with an ample source of motivation that led us to successfully write this paper.

Reference

[1] Sahare B and Naik A, Study Of Ethical Hacking, International Journal Of Computer Science Trends and Technology (IJCST), Vol 2 (Issue 4), Nov-Dec 2014

[2] Pandey B, Singh A, Balani L ,Ethical Hacking (Tools, Techniques & Approaches), International Conference on Advancement in IT and Management, DOI:10.13140/2.1.4542/2884, January 2015

[3] Patil S, Jagra A, Bhale M, Raina A, Kulkarni P, Ethical Hacking: The need for cyber security, IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), January 2017

[4] Satapathy S, Patra R, Ethical Hacking, International Journal of Scientific and Research Publications, Volume 5, Issue 6, June 2015

[5] Pinto M, Stuttard D, The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws, Wiley Publishing Inc., ISBN:978-0-470-17077-9, Page 2-13, 2008

[6] Baloch R, Ethical Hacking and Penetration Testing Guide, Taylor & Francis Group, ISBN:978-1-4822-3161-8, Page no 1-10, 2015

[7] Erickson J, Hacking: The Art of Exploitation, No Starch Press, ISBN**:** 978-1593271442, Page no 1-15, 2003