Ethical Hacking: The Need for Cyber Security

Indra Kumar Sahu

Department of Computer Science & Engineering,
Amity School of Engineering & Technology, Amity University Chhattisgarh

---***---

Hacking is basically expertise in any field. Hackers are classified as per working and as per knowledge. The ethical hackers come under white hat hackers. Ethical hackers use hacking techniques in order to provide security. They are legally authorized hackers. Various tools are used in order to carry out hacking. The most common hacking technique used is phishing. Since, there is a rapid growth in the number of attacks, there is a need for people to learn ethical hacking concepts to secure themselves.

INTRODUCTION

The vast growth of Internet has brought many good things like electronic commerce, email, easy access to vast stores of reference material etc. As, with most technological advances, there is also other side: criminal hackers who will secretly steal the organization's information and transmit it to the open internet. These types of hackers are called black hat hackers. So, to overcome from these major issues, another category of hackers came into existence and these hackers are termed as ethical hackers or white hat hackers. So, this paper describes ethical hackers, their skills and how they go about helping their customers and plug up security holes. Ethical hackers perform the hacks as security tests for their systems. This type of hacking is always legal and trustworthy. In other terms ethical hacking is the testing of resources for the betterment of technology and is focused on securing and protecting IP systems. So, in case of computer security, these tiger teams or ethical hackers would employ the same tricks and techniques that hacker use but in a legal manner and they would neither damage the target systems nor steal information. Instead, they would evaluate the target system's security and report back to the owners with the vulnerabilities they found and instructions for how to remedy them. Ethical hacking is a way of doing a security assessment. Like all other assessments an ethical hack is a random sample and passing an ethical hack doesn't mean there are no security issues. An ethical hack's results are a detailed report of the findings as well as a testimony that a hacker with a certain amount of time and skills is or isn't able to successfully attack a system or get access to certain information. Ethical hacking can be categorized as a security assessment, a kind of training, a test for the security of an information technology environment. An ethical hack shows the risks an information technology environment is facing and actions can be taken to reduce certain risks or to accept them.

ABOUT HACKING

Hacking occurs when someone intentionally accesses a computer without authorization. The term is often used to refer to a person with detailed computer knowledge who commits the act to accomplish criminal acts. The act often damages property, spreads viruses and causes financial loss. The New Hacker`s Dictionary uses several definitions including someone who "enjoys exploring the details of programmable systems and how to stretch their capabilities," "programs enthusiastically (even obsessively)," and "enjoys the intellectual challenge of creatively overcoming or circumventing limitations."

ABOUT ETHICAL HACKING

Ethical hacking is also known as White hat Hacking or Penetration Testing. Ethical hacking involves an authorized attempt to gain unauthorized access to a computer system or data. Ethical hacking is used to improve the security of the systems and networks by fixing the vulnerability found while testing.

Ethical hackers improve the security posture of an organization. Ethical hackers use the same tools, tricks, and techniques that malicious hackers used, but with the permission of the authorized person. The purpose of ethical hacking is to improve the security and to defend the systems from attacks by malicious users.

TYPES OF ETHICAL HACKERS

Hacktivists

Hacktivism is hacking into a computer system illegally for a social or politically motivated reason. These hackers could just leave a large message on the main page of a website, or even disrupt traffic to a site altogether. Some people see this as a form of protest, and therefore as protected speech. The question is whether anybody in America would object if someone hacked into a website where pedophile congregate and left a message saying that pedophilia is wrong. Therein lies the moral debate on whether hacktivists are ethical or not.

Cyberwarrior

This is another gray area of ethical hacking. Whether or not this type of hacking is ethical is all in the eye of the beholder. Cyberwarriors are computer experts and hackers who participate in cyberwarfare, which are actions undertaken or sanctioned by a nation-state to infiltrate another country's networks or computers to cause disruption or damage.

Black Box Penetration Testers

This is a hacker who is hired by a person or company to actually infiltrate a computer network or system. The hacker will act as a malicious hacker, trying to find vulnerabilities in a system or network that would allow him to attack it. The black box penetration tester has no prior knowledge of the network or system he is trying to infiltrate. By finding vulnerabilities, he can advise the company of individual about what is needed to strenghten a website from future hacking.

White Box Penetration Testers

This is another type of hacker that is hired by a person or company to break into a computer network or system. The white box hacker is much like the black box hacker in that they both are legally breaking into these systems in an effort to help the person or company who hires them. The only difference between the two is that white box penetrators are given complete knowledge of the system or network they are infiltrating. The hacker simulates an attack from an insider of the organization.

Certified Ethical Hacker/Licensed Penetration Tester

These hackers perform the duties of black box and white box penetration testers. They look for vulnerabilities and weaknesses in systems and networks. These two certifications are given by the International Council of E-Commerce Consultants. All of these ethical hackers must be re-certified every three years.

The Advantages of Ethical Hacking

Protection Against Theft

If a hacker gets into an organization's systems, then the hacker could gain access to valuable information. The organization's intellectual property and sensitive client information are at risk. Hackers have been known to steal such information. If organizations want to protect against theft, they could schedule routine ethical hacking exercises to find out if any flaws exist in their systems. This makes them less vulnerable to outside hackers.

Protection from Lawsuits

The United States is a litigious society. If hackers get into a company's systems and steal customer information, then the company could face potential lawsuits. Consumers could file lawsuits against an organization for failing to safeguard their personal information. Ethical hacking could help prevent the possibility of such lawsuits. Organizations may also have to meet certain legislative and regulatory requirements relating to safety of consumer information. Ethical hacking helps them meet such mandates.

CONCLUSIONS

To conclude, ethical hacking is a way of proceeding that puts the experience and work of cybersecurity professionals at the service of organisations. Its aim is to build systems that are strongly protected against malicious attacks. To achieve this, systems and servers are attacked in order to improve them.