International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 11 Issue 1 –NOVEMBER 2014.

Ethical Hacking Commandments

V. Prameela Rani

Lecturer, Dept of Computer Science, KBN College, Vijayawada, Andhra Pradesh, India

prameelarani.v@gmail.com

***Abstract*— The state of security on the internet is bad and getting worse. One reaction to this state of affairs is termed as Ethical Hacking which attempts to increase security protection by identifying and patching known security vulnerabilities on systems owned by other parties. As public and private organizations migrate more of their critical functions to the Internet, criminals have more opportunity and incentive to gain access to sensitive information through the Web application. 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. So, Ethical hacking is an assessment to test and check an information technology environment for possible weak links and vulnerabilities. Ethical hacking describes the process of hacking a network in an ethical way, therefore with good intentions. This paper describes what ethical hacking is, what it can do, an ethical hacking methodology as well as some commandments which can be used for an ethical hack.**

I. Definition

Ethical hacking refers to the act of locating weaknesses and vulnerabilities of computer and information systems by duplicating the intent and actions of malicious hackers. Ethical hacking is also known as penetration testing, intrusion testing, or red teaming. An ethical hacker is a security professional who applies their hacking skills for defensive purposes on behalf of the owners of information systems.

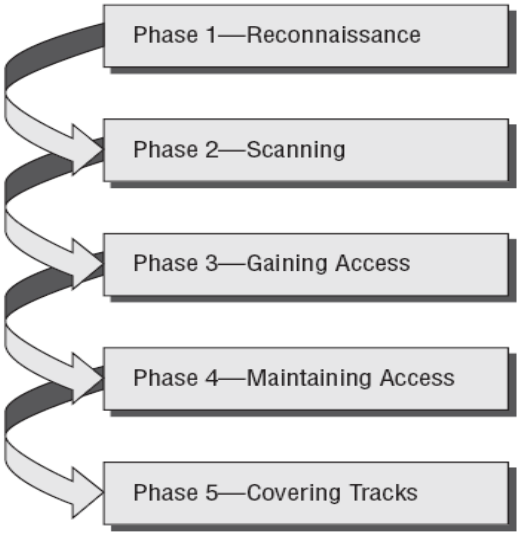
An Ethical Hacker, also known as a whitehat hacker, or simply a whitehat, is a security professional who applies their hacking skills for defensive purposes on behalf of the owners of information systems. Nowadays, certified ethical hackers are among the most sought after information security employees in large organizations such as Wipro, Infosys, IBM, Airtel and Reliance among others.

II. 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 focussed 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 is 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.

III. The Ethical Hacking Process

Ethical hackers must follow a strict scientific process in order to obtain useable and legal results.



Planning

Planning is essential for having a successful project. It provides an opportunity to give critical thought to what needs to be done, allows for goals to be set, and allows for a risk assessment to evaluate how a project should be carried out.

There are a large number of external factors that need to be considered when planning to carry out an ethical hack. These factors include existing security policies, culture, laws and regulations, best practices, and industry requirements. Each of these factors play an integral role in the decision making process when it comes to ethical hacking. The planning phase of an ethical hack will have a profound influence on how the hack is performed and the information shared and collected, and will directly influence the deliverable and integration of the results into the security program.

The planning phase will describe many of the details of a controlled attack. It will attempt to answer questions regarding how the attack is going to be supported and controlled, what the underlying actions that must be performed and who does what, when, where, and for how long.

Reconnaissance

Reconnaissance is the search for freely available information to assist in an attack. This can be as simple as a ping or browsing newsgroups on the Internet in search of disgruntled employees divulging secret information or as messy as digging through the trash to find receipts or letters.

Reconnaissance can include social engineering, tapping phones and networks, or even theft. The search for information is limited only by the extremes at which the organization and ethical hacker are willing to go in order to recover the information they are searching for.

The reconnaissance phase introduces the relationship between the tasks that must be completed and the methods that will need to be used in order to protect the organization's assets and information.

Enumeration

Enumeration is also known as network or vulnerability discovery. It is the act of obtaining information that is readily available from the target's system, applications and networks. It is important to note that the enumeration phase is often the point where the line between an ethical hack and a malicious attack can become blurred as it is often easy to go outside of the boundaries outlined in the original attack plan.

In order to construct a picture of an organization's environment, several tools and techniques are available. These tools and techniques include port scanning and NMap. Although it is rather simple to collect information, it is rather difficult to determine the value of the information in the hands of a hacker.

At first glance, enumeration is simple: take the collected data and evaluate it collectively to establish a plan for more reconnaissance or building a matrix for the vulnerability analysis phase. However, the enumeration phase is where the ethical hacker's ability to make logical deductions plays an enormous role.

Vulnerability Analysis

In order to effectively analyze data, an ethical hacker must employ a logical and pragmatic approach. In the vulnerability analysis phase, the collected information is compared with known vulnerabilities in a practical process.

Information is useful no matter what the source. Any little bit can help in discovering options for exploitation and may possibly lead to discoveries that may not have been found otherwise. Known vulnerabilities, incidents, service packs, updates, and even available hacker tools help in identifying a point of attack. The Internet provides a vast amount of information that can easily be associated with the architecture and strong and weak points of a system.

Exploitation

A significant amount of time is spent planning and evaluated an ethical hack. Of course, all this planning must eventually lead to some form of attack. The exploitation of a system can be as easy as running a small tool or as intricate as a series of complex steps that must be executed in a particular way in order to gain access.

The exploitation process is broken down into a set of subtasks which can be many steps or a single step in performing the attack. As each step is performed, an evaluation takes place to ensure that the expected outcome is being met. Any divergence from the attack plan is classified into two determinations:

Expectations: Are the expectations of the exploitation being met or are the results conflicting with the organization's assumptions?

Technical: Is the system reacting in an unexpected manner, which is having an impact on the exploitation and the engagement as a whole?

Final Analysis

Although the exploitation phase has a number of checks and validations to ensure success, a final analysis is required to categorize the vulnerabilities of the system in terms of their level of exposure and to assist in the derivation of a mitigation

plan. The final analysis phase provides a link between the exploitation phase and the creation of a deliverable.

A comprehensive view of the entire attack must exist in order to construct a bigger picture of the security posture of the environment and express the vulnerabilities in a clear and useful manner. The final analysis is part interpretation and part empirical results.

Deliverables

Deliverables communicate the results of tests in numerous ways. Some deliverables are short and concise, only providing a list of vulnerabilities and how to fix them, while others are long and detailed, providing a list of vulnerabilities with detailed descriptions regarding how they were found, how to exploit them, the implications of having such vulnerability and how to remedy the situation.

The deliverable phase is a way for an ethical hacker to convey the results of their tests. Recently, ethical hacking has become so commoditized that if a deliverable does not instill fear into the hearts of executives, it could be considered a failure.

Integration

Finally, it essential that there is some means of using the test results for something productive. Often, the deliverable is combined with existing materials, such as a risk analysis, security policy, previous test results, and information associated with a security program to enhance mitigation and develop remedies and patches for vulnerabilities.

There are three distinguishing factors that should be considered during the integration of any test results:

Mitigation: If vulnerability beyond acceptable risk was found, then it would need to be fixed. Mitigation of vulnerability can include testing, piloting, implementing, and validating changes to systems.

Defense: Vulnerabilities need to be addressed in a strategic manner in order to minimize future or undetected vulnerabilities. Defense planning is establishing a foundation of security to grow on and ensure long-term success.

Incident Management: The ability to detect, respond, and recover from an attack is essential. Knowing how attacks are made and the potential impacts on the system aids in formulating an incident response plan. The ethical hacking process provides an opportunity for discovering the various weaknesses and attractive avenues of attack of a system which can aid in preventing future attacks.

IV. The Ten Commandments

Becoming a believer in the doctrine of ethical hacking, requires that one following the 10 Commandments of Ethical Hacking described below:

1. Thou shalt set thy goals

An ethical hacker should set simple goals, such as finding unauthorized wireless access points or obtaining information from a wired network system. In any case, the goals should be articulate and well communicated.

2. Thou shalt plan thy work, lest thou go off course

Ethical hackers are bound by constraints. Consequently, it is important to develop a strategy plan which should include identifying the networks to test, specifying the testing interval, specifying the testing process, and obtaining approval of the plan.

3. Thou shalt obtain permission

Written permission is required and should state that an ethical hacker is authorized to perform a test according to the plan. It should also say that the organization will provide legal and organizational support in case criminally charges or lawsuits arise. This is conditional on staying within the bounds of the approved plan.

4. Thou shalt work ethically

An ethical hacker is bound to confidentiality and non-disclosure of information they may uncover. Ethical hackers must also be compliant with their organization's governance and local laws. An ethical hack must not be performed when the company policy or the law for that matter, explicitly forbids it.

5. Thou shalt keep records

Patience and thoroughness are attributes of a good ethical hacker. A hallmark of ethical hacker professionalism is keeping adequate records to support findings. The date and details regarding each test, whether or not they were successful, should be logged and recorded and a duplicate copy of the log book should be kept.

6. Thou shalt respect the privacy of others

An ethical hacker must not abuse their authority. Ethical hackers must snoop into confidential corporate records or private lives. The information that is uncovered should be treated with the same care one would give to their own personal information.

7. Thou shalt do no harm

The actions of an ethical hacker may have unplanned repercussions. It is easy to get caught up in the work and cause a denial of service or trample on someone else's rights. It is important to stick to the original plan.

8. Thou shalt use a scientific process

The work of an ethical hacker should adopt an empirical method. An empirical method will help set quantifiable goals, develop consistent and repeatable tests, and provide tests that are valid in the future.

9. Thou shalt not covet thy neighbour's tools

Ethical hackers will always discover new tools to help them get their job done. Tools are abundant on the Internet and more are coming out all the time. The temptation to grab them all is fierce. Although it is possible to use all of the tools that are available, it is recommended that an ethical hacker choose one and stick with it.

10. Thou shalt report all thy findings

Ethical hackers should plan to report any high-risk vulnerabilities discovered during testing as soon as they are

found. Reports are one way for the organization to determine the completeness and thoroughness of the work of an ethical hacker and provide a means for peers to review methodologies, findings, analysis, and conclusions.

V. REFERENCES

[1] http://wiki.cas.mcmaster.ca/index.php/Ethical_Hacking
[2] http://www.ijirset.com/upload/2013/december/62_ETHICAL.pdf
[3] http://www.dummies.com/how-to/content/obeying-the-ten-commandments-of-ethical-hacking.html
[4] http://en.wikipedia.org/wiki/TenCommandmentsofComputerEthics CEH(Certified Ethical Hackers)2010V6.
[5] Hacking Wireless Networks For Dummies.
[6] Ethical Hacking and Countermeasures- Web Applications and Data Servers.
[7] HACKING: THE ART OF EXPLOITATION