International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 01 | Jan-2018 www.irjet.net p-ISSN: 2395-0072

Ethical Hacking

Sountharraj.A.C [1], Barath.A [2]

[1]Assistant Professor, Department of BCA & M.Sc SS, Sri Krishna Arts and Science College, Tamilnadu, India
[2]III BCA, Department of BCA & M.Sc SS, Sri Krishna Arts and Science College, Tamilnadu, India

---

Abstract - *The primary target of this paper is to give a complete report on Ethical Hacking. The explosive growth of the Internet has brought many good things: e-commerce, collaborative computing, e-mail, and new avenues for advertising and information distribution, to name a few. Hacking is the act of finding the possible entry points that exist in a computer system or a computer network and finally entering into them to collect data. Hacking is an attempt to exploit a computer system and a private network inside a computer. It is the unauthorized access to or control over computer network security systems for some illicit purpose. Hackers are usually a skilled programmers with the knowledge of computer security. Ethical hackers are becoming a mainstay of the effort to make corporate networks more secure. The Ethical hacker hacks into a computer network in order to evaluate and improve its security rather than with criminal intent.*

***Key Words*: Hacker, Penetration, Ethical, Hacks.**

1. INTRODUCTION

Hacking has been a part of computing for almost five decades and it is a very broad discipline, which covers a wide range of topics. The first known event of hacking had taken place in 1960 at MIT and at the same time, the term "Hacker" was originated. In this report, we will take you through the various concepts of Ethical Hacking and explain how you can use them in a real-time environment.

1.1 HISTORY OF ETHICAL HACKING

In point of fact, the first hackers appeared in the 1960's at the Massachusetts Institute of Technology (MIT), and their first victims were electric trains. They wanted them to perform faster and more efficiently. In 1964 "Tiger Teams" as a group of technical specialists selected for their experience, energy and imagination. One of the first teams was assigned to track down possible sources of failure in a spacecraft subsystem. In 1974 the U.S. Air Force conducts one of the first ethical hacks, a security hacks, a security evaluation of the Multics operating system. In 2009 Penetration Testing Execution Standard (PTES) launches, offering business and security service providers a common language and scope for performing penetration tests. In 2013 Worldwide enterprise security spending reaches $6.4 billion.

2. THE ETHICAL HACKING PROCESS

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

2.1 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 ethical hack of this phase have a deep influence on how the hacking should be performed and the information shared and collected, and will directly influence the deliverable and integration of the results into the security program of it.

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.

2.2 RECONNAISSANCE

Reconnaissance is the search for freely available information in a network or server 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 is the phase where the attacker gathers all information about a specific target. The tools that are widely used in this process to protect are NMAP, Maltego, and Google Dorks. The reconnaissance phase introduces the relationship between the tasks that must be completed and the methods that will need to be used in to protect the organization's assets and information.

2.3. 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 totally 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 each time. The Internet provides a vast amount of information that can easily be associated with the architecture and strong and weak points of a system.

2.4. EXPLOITATION

A significant amount of time is spent for planning because it is evaluated by ethical hack. Surely, all this planning must eventually lead to some form of attack. The exploitation of a system can be as easy to run 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 or parts 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.

2.4. FINAL ANALYSIS

Although the exploitation phase has a number of checks and validations to ensure success, a final analysis is required to categorize it. 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 two things 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.

2.5. DELIVERABLES

Deliverables communicate the results of tests in several ways. Some deliverables are short and brief, 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 and how to exploit them, the implications of having such a vulnerability and how to remedy the situation.

The deliverable phase is the only way for an ethical hacker to convey the results of their tests. Recently, ethical hacking has having economic value.

2.6. INTEGRATION

Finally, it is essential that there is some means of using the test results for something productive. Often, the deliverable is combined with existing materials of it, 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.

3. TYPES OF ETHICAL HACKING

Ethical hackers use various methods for breaking the security system in the organizations in the period of cyberattack from other side. Various types of ethical hacks are:

- ***Remote Network:*** This process in especially utilized to recognize the attacks that are causing among the internet. Usually the ethical hacker always tries to identify the default and proxy information into the networks some of them are firewalls, proxy etc.

- ***Remote Dial Up Network:*** Remote dial up network hack identify and try to protest from the attack that is causing among the client modern pool. For finding the open system the organizations will make use of the method called war dialling for the representative dialling. Open system is one of the examples for this type of attacks.

- ***Local Network:*** local network hack is the process which is used to access the illegal information from authorized network by making use of someone with physical access gaining through the local network. To start on this procedure the ethical hacker should ready to access the local network directly.

- ***Stolen Equipment:*** By making use of the stolen equipment hack it is easy to identify the information of the thefts such as the laptops, hard disk etc. the information secured by the owner of the laptop can be identified (Kimberly graves, 2007). Information like username, password and the security settings that are in the equipment are encoded by stealing the laptop.

- ***Social Engineering:*** A social engineering attack is the process which is used to check the reliability of the organization; this can be done by making use of the telecommunication or face to face communication by collecting the data which can be used in the attacks (Bryan Foss and Merlin Stone, 2002). This method is especially utilized to know the security information that is used in the organizations.

- ***Physical Entry:*** This Physical entry organization is used in the organizations to control the attacks that are obtained through the physical premises (Ronald l. Krutz and russel dean Vines, 2007). By using the physical

entire the ethical hacker can increase and can produce virus and other Trojans directly onto the network.

- ***Application Network:*** The logic flaws present in the applications may result to the illegal access of the network and even in the application and the information that is provided in the applications.

- ***Network Testing:*** In this process it mainly observes the unsafe data that is present in the internal and the external network, not only in the particular network also in the devices and including the virtual private network technologies

- ***Wireless Network Testing:*** In this process the wireless network reduces the network liability to the attacker by using the radio access to the given wireless network space.

- ***Code Review:*** This process will observe the source code which is in the part of the verification system and will recognize the strengths and the weakness of the modules that are in the software.

- ***War Dialling:*** It simply identifies the default information that is observed in the modem which is very dangerous to the corporate organizations.

WHAT CONSTITUTES ETHICAL HACKING?

For hacking to be allow ethically, the hacker must obey the following rules:

- Expressed (often written) permission to probe the network and attempt to identify potential security risks.

- You respect the individual's or company's privacy.

- You close out your work, not leaving anything open for you or someone else to exploit at a later time.

- You let the hardware manufacturer or software developer know the security vulnerabilities you can locate in their software or hardware, if not already known by the company.

5. ADVANTAGES OF ETHICAL HACKING.

Most of the benefits of ethical hacking are distinct, but many are unnoticed. The benefits range from simply preventing malicious hacking to preventing national security breaches. The benefits include:

- This prevents identity and the leaking of vital information.

- It allows them to implement stronger security measures.

- It is also beneficial to help government entities to protect major computer systems from being compromised in a way that national security would be an issue.

REFERENCES

[1] Ankit Fadia, "Network Security: A Hacker's Perspective", 2002.

[2] Ankit Fadia, "An Ethical Guide to Hacking Mobile Phones", 2005.

[3] R Rafay Baloch,"Ethical Hacking and Penetration Testing Guide", 2014.

[4] James Corley, Kent Backman, and Michael "Hands-On Ethical Hacking and Network Defence", 2006.