Ethical Hacking with Penetration Testing

Shivam [1], Namit Gupta [2]

[1] *Student, College of Computing Science & Information Technology TMU Moradabad 244001, Uttar Pradesh, INDIA*
[2] *Asst. Professors, College of Computing Science & Information Technology TMU Moradabad 244001, Uttar Pradesh, INDIA*

[1]shivamprajapati7037@gmail.com
[2]namit.k.gupta@gmail.com

Abstract— **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.**

Keywords— Hacking, Penetration Testing, Types, Features, Network Testing.

Fig.1. Ethical Hacking

I. Introduction

The increasingly growth of internet has given an entrance passage to many things : e-commerce , email , social networking , online shopping & information distribution. As the technology advances it has its dark side; hackers. Govt. organization , private citizen & many companies of the world wants to be the part of this revolution. Being afraid of hackers as they could break into the web-server & create nuisance. To counter attack them ethical hacker's are used in the Govt. organization, companies etc. This paper describes the skills, attitude & how they helps the customer with the increasingly growth rate of internet network security has been a measure concern of Govt.& private organization. As different organization wants to take advantage of the internet but fail to do so, because of the possibility of being hacked. To minimize the risk of being hacked by the hackers the organizations realized the best possible ways to introduced the independent computer security professionals to make their way out. In computer security the ethical hackers employ's some tools & techniques that would neither damaged the system nor still information from it. Instead they would evaluate ways to secure then system & report back the owner with the threat they had found & how to cure them.

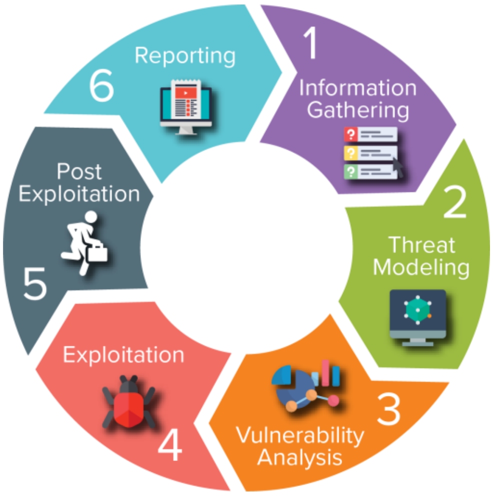

Fig.2. Penetration Testing Process

A. Hacking is not what we think , It is an art of exploring the threats in a system . Today it sounds something with negative shade , but it is not exactly that many professionals hack system so as to learn the deficiencies in them and to overcome from it and try to improve the system security. Hacking is not about breaking security of computer and network. Programmers, who know different computer languages very well, they themselves define as hackers, who are good at programming. Hacking in simple words: breaking into private party in silence and enjoy it. Which logically means trying to get into some ones private account or to steal the sensitive data and do things that are illegal? Ethical hackers are the people who can create a firewall according to your knowledge and needs and protect all weak spots to protect private data from being hacked. The word hacking is not illegal, computer programmers called themselves hackers because they can break into the system and solves the problem.

II. Types of hackers

There are six types of hackers:

A) **White Hat Hackers:** White Hat hackers are also known as Ethical Hackers. They never intent to harm a system, rather they try to find out weaknesses in a computer or a network system as a part of penetration testing and vulnerability assessments. Ethical hacking is not illegal and it is one of the demanding jobs available in the IT industry. There are numerous companies that hire ethical hackers for penetration testing and vulnerability assessments.

B) **Black Hat Hackers:** Black Hat hackers, also known as crackers, are those who hack in order to operations or steal sensitive information. Black Hat hacking is always illegal because of its bad intent which includes stealing corporate data, violating privacy, damaging the system, blocking network communication, etc.

C) **Grey Hat Hackers:** Grey hat hackers are a blend of both black hat and white hat hackers. They act without malicious intent but for their fun, they exploit a security weakness in a computer system or network without the owner's permission or knowledge. Their intent is to bring the weakness to the attention of the owners and getting appreciation or a little bounty from the owners.

D) **Red Hat Hackers:** Red hat hackers are again a blend of both black hat and white hat hackers. They are usually on the level of hacking government agencies, top-secret information hubs, and generally anything that falls under the category of sensitive information.

E) **Blue Hat Hackers:** A blue hat hacker is someone outside computer security consulting firms who is used to bug-test a system prior to its launch. They look for loopholes that can be exploited and try to close these gaps. Microsoft also uses the term **Blue Hat** to represent a series of security briefing events.

F) **Elite Hackers:** This is a social status among hackers, which is used to describe the most skilled. Newly discovered exploits will circulate among these hackers.

III. FEATURES OF ETHICAL HACKING

Information is meaningful data which has to be protected in order to protect the privacy, security, identity of an organization or a person or a nation. An information is called valuable because of few characteristics. The main characteristics which make an information valuable are :

1. **Confidentiality:** Confidentiality ensures that an Information is accessible to only an authorized user. The main purpose of confidentiality is to protect the sensitive information from reaching the wrong hands. It is used to maintain the privacy of the people. Encryption is a good example of confidentiality.

2. **Availability:** Information should be available to an authorised person when it is requested for. It is the guarantee of access to the authorised individual to information. Keeping all the hardware and software up to date and keeping back up, taking proper recovery measures will ensure availability of data.

3. **Integrity:** Integrity maintains the correctness or accuracy of the information while the data is in transit, storage or processing. It is the guarantee that information is trust worthy and not tampered. This attribute ensures that an unauthorised person will not be able to modify the data.

4. **Authentication:** It is verifying whether the user, data, transactions involved is genuine. This attribute ensures that only genuine or right people are given access to the information. Login mechanisms can be used to verify the authenticity of users.

5. **Non-Repudiation:** This is a property of information which is used to holds a person responsible for the information he sent or received. In future, he cannot deny his role in sending or receiving the information.

IV. NETWORK PENETRATION TESTING AND EXPLOITATION

After the penetration tester performs Intelligence gathering and threat modeling, the tester completes a series of network tests. Network testing is usually the most common method of penetration testing. Once a hacker obtains access to the network, 90% of the obstacles are removed for a threat actor.

A pentester can conduct internal and external network exploitation. This allows them to emulate a successful hacker that’s been able to penetrate the external network defenses. This gives them an opportunity to explore many facets of the security posture of an organization.

Network Testing Typically includes:

- Bypassing Firewalls
- Router testing
- IPS/IDS evasion
- DNS footprinting
- Open port scanning and testing
- SSH attacks
- Proxy Servers
- Network vulnerabilities
- Application penetration testing

Website and Wireless Network Penetration Testing:

Through this penetration test type, the devices and infrastructure within the wireless network are tested for vulnerabilities.

1) The pentester will commonly exploit these areas during a wireless network penetration test:

A) Wireless encryption protocols.
B) Wireless network traffic.
C) Unauthorized access points and hotspots.
D) MAC address spoofing.
E) Poorly used or default passwords.
F) Cross-site scripting.
G) SQL injections.
H) Denial of Service (DoS) attacks.
I) Web server misconfiguration.
J) The website and/or web server for sensitive customer data.
K) The web server(s) using malware to obtain deeper access into your network.

V. LIMITATIONS OF ETHICAL HACKING

- Ethical hacking is based on the simple principle of finding the security vulnerabilities in systems and networks before the hackers do, by using so-called “hacker” techniques to gain this knowledge. Unfortunately, the common definitions of such testing usually stop at the operating systems, security settings, and “bugs” level. Limiting the exercise to the technical level by performing a series of purely technical tests, an ethical hacking exercise is no better than a limited “diagnostic” of a system’s security.

- Time is also a critical factor in this type of testing. Hackers have vast amounts of time and patience when finding system vulnerabilities. Most likely you will be engaging a “trusted third party” to perform this test for you, so to you time is money. Another consideration in this is that in using a “third party” to conduct you tests, you will be providing “inside information” in order to speed the process and save time. The opportunity for discovery may be limited since the testers may only work by applying the information they have been given.

VI. CONCLUSION

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.

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. Hacking is usually done to gain unauthorized access to a computer system or a computer network, either to harm the systems or to steal sensitive information available on the computer. 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 what we call **Ethical Hacking**.

VII. REFERENCE

1]. <http://tlc.discovery.com/convergence/hackers/articles/history.html>. Stallman, Richard.

2]. “The GNU Manifesto.” The New Media Reader. Eds. Noah Wardrip-Fruin and Nick Môn fort.
Cambridge: MIT Press, 2003. Sterling, Bruce.
3]. CyberTerrorism. Online. Discovery Communications.

28Oct.2003.<http://tlc.discovery.com/convergence/hackers/articles/cyberterror.html> Quittner, Jeremy.

4]. Wikipedia
5]. Tutorial point.
6]. Gurpreet K. Juneja,”Ethical hacking :A technique to enhance information security”international journal of computer applications(3297: 2007),vol. 2,Issue 12,december2013.