IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Concepts Of Ethical Hacking: A Survey

[1]Rajesh Durganath, [2]Varun Totakura, [3]Bhavani Anil Goud, [4]M. I. Thariq Hussan

[123]Student Scholar, [4]Professor & Head of Department

[134]Department of Information Technology, [2]Department of Computer Science and Engineering

[1234]Guru Nanak Institutions Technical Campus, Hyderabad, India

Abstract: Electronic commerce is an easy access to vast stores of reference material, collaborative computing, e-mail, and new avenues for advertising and information distribution. The government concerns, private companies and even individual citizens around the world are anxious to be a part of this revolution, but they are afraid that some hacker will break into their web server and replace their logo with pornography, read their e-mail, steal their credit card number from an on-line shopping site, or implant software that will secretly transmit their organization's secrets to the open internet. With these concerns the ethical hacker can help. In this article, hacker skills, their attitudes, and how they go about helping their customers to find and plug up the security holes. The ethical hacking process is explained, along with many of the problems that the Global Security Analysis lab has seen during its early years of ethical hacking for IBM clients**.**

Index Terms **- Ethical Hacking, Hacker.**

I. INTRODUCTION

Hacking is identifying the weakness in computer systems or networks to exploit its weaknesses to gain access. Example of Hacking: Using password cracking algorithm to gain access to a system. Computers have become mandatory to run a successful business. It is not enough to have isolated computers systems they need to be networked to facilitate communication with external businesses. This exposes them to the outside world and hacking. Hacking means the using of computers to commit fraudulent acts such as fraud, privacy invasion, stealing corporate/personal data, etc. Cybercrimes cost many organizations millions of dollars every year. Businesses need to protect themselves against such attacks.

- WHITE HAT HACKING

White Hat Hacking refers to hacking which is done to protect networks or say computers from black hat hackers or (who hacks for their personal means). White Hat Hacking is done for security purpose or to test security programs. White hat hacking also refers to ethical hacking. Those white hat hackers are also known as ethical hackers and hack for non-malicious reasons. They have defined code of ethics and often work with manufacturer to get accurate weakness.

- BLACK HAT HACKING

Black Hat Hacking violates a computer or network or network security for some personal gain or for some type of challenges. Black hat hacking is illegal because the black hat hacker gain access to systems without enough security permissions and use it as way he/she wants. The person who perform black hat hacking is termed as black hat hacker. They gain access to systems and make it unusable for others by destroying its inner maintenance.

II. CONCEPTS OF ETHICAL HACKING

- PHASE OF PENTESTING

Penetration testing (also called pen testing) is the practice of testing a computer system, network or web application to find vulnerabilities that an attacker could exploit. Pen tests can be automated with software applications or they can be performed manually. Either way, the process includes gathering information about the target before the test (reconnaissance), identifying possible entry points, attempting to break in (either virtually or for real) and reporting back the findings.

- FOOT PRINTING

Tools and tricks to get the information about the computer, IP and MAC address related to the user and system.

- SCANNING

Before starting the pen testing, pen tester must have some information about network and system. So, pen tester scans the entire network with some tools like Nmap, Zenmap, ping and hping etc.

- ENUMERATION

During the enumeration phase, possible entry points into the tested systems are identified. The information collected during the reconnaissance phase is put to use.

- SYSTEM HACKING

System hacking can login to system without credentials not only bypass the credentials but also you can work in the system as root user by privilege escalation.

- TROJANS

It is a generally non-self-replicating type of malware program containing malicious code. A Trojan often acts as a backdoor, contacting a controller which can then have unauthorized access to the affected computer While Trojans and backdoors are not easily detectable by themselves, computers may appear to run slower due to heavy processor or network usage.

- VIRUS AND WORMS

A computer virus attaches itself to a program or file enabling it to spread from one computer to another, leaving infections. A worm is its capability to replicate itself on your system, so rather than your computer sending out a single worm, it could send out hundreds or thousands of copies of itself, creating a huge devastating effect.

- SNIFFING TRAFFIC

It is a program that monitors and analyzes network traffic, detecting and finding problems. Various technique and tools used for sniffing like kali, linux, MITM attack, tshark, urlsnarf etc.

- SOCIAL ENGINEERING

In this technique, the ethical hacker create the phishing page of website to obtain credential of users.

- DENIAL OF SERVICE

A DOS attack generally consists of efforts to temporarily interrupt or suspend or down the services of a host connected to the Internet.

III. HACKING PHASES

The hacking consists of five phase which has been illustrated in the following Figure. 1.

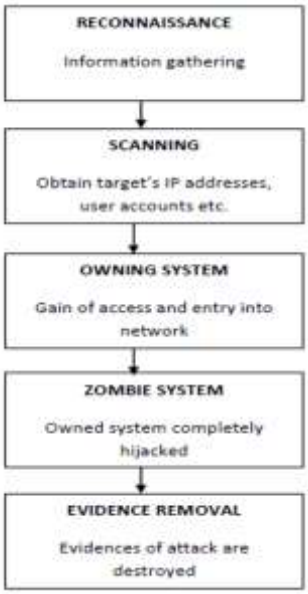

Fig 1. Hacking Phases

- RECONNAISSANCE

It can be active or passive. In the passive reconnaissance, the information is gathered regarding the target without knowledge of targeted company (or individual). It could be done simply by searching information of the target on internet or bribing an employee of targeted company who would reveal and provide useful information to the hacker.

This process is also called as "information gathering". In this approach, the hacker does not attack the system or network of the company to gather information. Whereas in active reconnaissance, the hacker enters into the network to discover individual hosts, IP addresses and network services. This process is also called as "rattling the doorknobs". In this method, there is a high risk of being caught as compared to passive reconnaissance.

- SCANNING

In the scanning phase, the information gathered in phase 1 is used to examine the network. Tools like dialers, port scanners etc. are being used by the hacker to examine the network so as to gain entry in the company's system and network.

- OWINING THE SYSTEM

This is the real and actual hacking phase. The hacker uses the information discovered in earlier two phases to attack and enter into the local area network (LAN, either wired or wireless), local PC access, internet or offline. This phase is also called as "owning the system".

- ZOMBIE SYSTEM

Once the hacker has gained the access in the system or network, he maintains that access for future attacks (or additional attacks), by making changes in the system in such a way that other hackers or security personals cannot then enter and access the attacked system. In such a situation, the owned system (mentioned in Phase 3) is then referred to as "Zombie System".

- EVIDENCE REMOVAL

In this phase, the hacker removes and destroys all the evidences and traces of hacking, such as log files or intrusion detection system alarms, so that he could not be caught and traced. This also saves him from entering into any trial or legality. Now, once the system is hacked by hacker, there is several testing methods available called penetration testing to discover the hackers and crackers.

IV. BENEFITS OF ETHICAL HACKING

This type of "test" can provide convincing evidence of real system or network level threat exposures through proof of access. Even though these findings may be somewhat negative, by identifying any exposure you can be proactive in improving the overall security of your systems.

However, information security should not be strictly limited to the mechanics of hardening networks and computer systems. A mature security information program is a combination of policies, procedures, technical system and network standards, configuration settings, monitoring, and auditing practices. Business systems, which have resisted simple, direct attacks at the operating system or network level, may succumb to attacks that exploit a series of procedural, policy, or people weak points.

An ethical hack, which tests beyond operating system and network vulnerabilities, provides a example, should your ethical hack prove that your firewalls could withstand an attack because there was no breach, but no one noticed the attacks, you may be better prepared to make a case for improving intrusion detection broader view of an organization's security. The results should provide a clear picture of how well your detection processes works as well as the response mechanisms that should be in place. "Tests" of this sort could also identify weakness such as the fact that many systems security administrators may not be as aware of hacking techniques as are the hackers they are trying to protect against. These findings could help promote a need for better communication between system administrators and technical support staff, or identify training needs.

Quite often, security awareness among senior management is seriously lacking. Traditional diagnostic work primarily deals with the possibility of a threat and this often leads to a casual view of the threat, deferring the need to immediately address the requirements. Through an ethical hacking exercise especially if the results are negative, senior management will have a greater understanding of the problems and be better able to prioritize the requirements for improving intrusion detection.

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 definition of such testing usually stops 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. 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.

A further limitation of this type of test is that it usually focuses on external rather than internal areas; therefore, you may only get to see half of the equation. If it is not possible to examine a system internally, how can it be established that a system is "safe from attack", based purely upon external tests? Fundamentally this type of testing alone can never provide absolute assurances of security. Consequently, such assessment techniques may seem, at first, to be fundamentally flawed and have limited value, because all vulnerabilities may not be uncovered.

VI. TYPES OF ATTACKS

- SNOOPING

This is when someone looks through your files in the hopes of finding something interesting whether it is electronic or on paper. In the case of physical snooping people might inspect your dumpster, recycling bins, or even your file cabinets; they can look under your keyboard for post-It-notes, or look for scraps of paper tracked to your bulletin board. Computer snooping on the other hand involves someone searching through your electronic files trying to find something interesting.

- INTERCEPTION

This can be either an active or passive process. In a networked environment, a passive interception might involve someone who routinely monitors network traffic. Active interception might include putting a computer system between sender and receiver to capture information as it is sent. From the perspective of interception, this process is covert. The last thing a person on an intercept mission wants is to be discovered. Intercept missions can occur for years without the knowledge of the intercept parties.

- MODIFICATION ATTACKS

This involves the deletion, insertion, or alteration of information in an unauthorized manner that is intended to appear genuine to the user. These attacks can be very hard to detect. The motivation of this type of attack may be to plant information, change grades in a class, alter credit card records, or something similar. Website defacements are a common form of modification attacks.

- REPUDIATION ATTACKS

This makes data or information to appear to be invalid or misleading (Which can even be worse). For example, someone might access your email server and inflammatory information to others under the guise of one of your top managers. This information might prove embarrassing to your company and possibly do irreparable harm. This type of attack is fairly easy to accomplish because most email systems don't check outbound email for validity. Repudiation attacks like modification attacks usually begin as access attacks.

- DENIAL OF SERVICE ATTACKS

They prevent access to resources by users by users authorized to use those resources. An attacker may try to bring down an e-commerce website to prevent or deny usage by legitimate customers. DOS attacks are common on the internet, where they have hit large companies such as Amazon, Microsoft, and AT&T. These attacks are often widely publicized in the media. Several types of attacks can occur in this category. These attacks can deny access to information, applications, systems, or communications. A DOS attack on a system crashes the operation system (a simple reboot may restore the server to normal operation). A common DOS attack is to open as many TCP sessions as possible, this type of attack is called TCP SYN flood DOS attack. Two of the most common are the ping of death and the buffer overflow attack. The ping of death operates by sending Internet control message protocol (ICMP) packets that are larger than the system can handle. Buffer overflow attacks attempt to put more data into the buffer than it can handle. Code red, slapper and slammer are attacks that took advantage of buffer overflows.

- DISTRIBUTED DENIAL OF SERVICE ATTACKS

This is similar to a DOS attack. This type of attack amplifies the concepts of DOS attacks by using multiple computer systems to conduct the attack against a single organization. These attacks exploit the inherent weaknesses of dedicated networks such as DSL and Cable. These permanently attached systems have little, if any, protection. The attacker can load an attack program onto dozens or even hundreds of computer systems that use DSL or Cable modems. The attack program lies dormant on these computers until they get attack signal from the master computer. This signal triggers these systems which launch an attack simultaneously on the target network or system.

- BACKDOOR ATTACKS

This can have two different meanings, the original term back door referred to troubleshooting and developer hooks into systems. During the development of a complicated operating system or application, programmers add back doors or maintenance hooks. These back doors allow them to examine operations inside the code while the program is running. The second type of back door refers to gaining access to a network and inserting a program or utility that creates an entrance for an attacker. The program may allow a certain user to log in without a password or gain administrative privileges. A number of tools exist to create a back door attack such as, Back Orifice (Which has been updated to work with windows server 2003 as well as earlier versions), Subseven, NetBus, and NetDevil. There are many more. Fortunately, most anti-virus software will recognize these attacks.

- SPOOFING ATTACKS

This is an attempt by someone or something to masquerade as someone else. This type of attack is usually considered as an access attack. The most popular spoofing attacks today are IP spoofing and DNS spoofing. The goal of IP spoofing is to make the data look like it came from a trusted host when it really didn't. With DNS spoofing, The DNS server is given information about a name server that it thinks is legitimate when it isn't. This can send users to a website other than the one they wanted to go to.

- MAN-IN-THE-MIDDLE ATTACKS (MITM)

This type of attack is also an access attack, but it can be used as the starting point of a modification attack. This involves placing a piece of software between a server and the user that neither the server administrators nor the user are aware of. This software intercepts data and then sends the information to the server as if nothing is wrong. The server responds back to the software, thinking it's communicating with the legitimate client. The attacking software continues sending information to the server and so forth.

- REPLAY ATTACKS

This occurs when information is captured over a network. Replay attacks are used for access or modification attacks. In a distributed environment, logon and password information is sent over the network between the client and the authentication system. The attacker can capture this information and replay it later. This can also has security certificates from systems such as kerberos: The attacker resubmits the certificate, hoping to be validated by the authentication system, and circumvent any time sensitivity.

- PASSWORD GUESSINGATTACK

This occurs when an account is attacked repeatedly. This is accomplished by sending possible passwords to an account in a systematic manner. These attacks are initially carried out to gain passwords for an access or modification attack.

VII. NEED OF ETHICAL HACKERS

A product security engineer at FlipKart, recently won a whopping USD 15000 for reporting major security flaws in Facebook, Twitter and many other companies. Not just Anand, many qualified technocrats are entering into ethical hacking space with an aim to make it as a full-time profession. Today, there is a huge demand for ethical hackers in the market, who can not only safeguard the enterprises from organized cybercrime groups but assist them to assess their cyber security preparedness. While countries such as the USA and UK are far ahead in utilizing ethical hackers in a best way, countries like India is yet to change its perspective about the concept of white hat hackers.

According to Data Security Council of India, the cyber security market is expected to grow to USD 35 billion by 2025. A report by NASSCOM states that the country needs at least one million skilled people by 2020. These figures are clear indication that the country has a huge scarcity of qualified cyber security professionals and the need is going to become severe with cyber criminals increasingly targeting enterprises and government establishments.

VIII. TOP FIVE ETHICAL HACKERS

1. Rishiraj Sharma is from Mumbai who became an ethical hacker at the age of 16.

2. Ankit Fadia is an Indian author, speaker, television host, and self-proclaimed "ethical hacker" of computer systems, whose skills and ethics have been debated. His work mostly involves OS and Networking based tips and tricks, proxy websites and lifestyle.

3. Sunny Vaghela is one of the countries pioneer Information Security & Cyber Crime Consultant. The young and dynamic personality of Sunny has not only assisted in solving complex cybercrime cases but has also played an instrumental role in creating awareness about information security and cybercrimes.

4. Rahul Tyagi is a student of Lovely Professional University and has been selected as Brand Ambassador of a well-reputed IT Company TCIL functioning at Chandigarh. He has to act for corporate ethical hacking module.

5. Sai Satish is a young Entrepreneur, Founder & CEO of Indian Servers. He is the Administrator of Andhrahackers (Top hacking awareness forum in INDIA).

IX. CONCLUSION

Hackers are very diverse and they may bankrupt a company or may protect the data, increasing the revenues for the company. The battle between the ethical or white hat hackers and the malicious or black hat hackers is a long war, which has no end. While ethical hackers help to understand the companies' their security needs, the malicious hackers intrude illegally and harm the network for their personal benefits, which may allow a malicious hacker to breach their security system. Ethical Hackers help organizations to understand the present hidden problems in their servers and corporate network. Ethical Hacking is a tool, which if properly utilized, can prove useful for understanding the weaknesses of a network and how they might be exploited. This also concludes that hacking is an important aspect of computer world. It deals with both sides of being good and bad. Ethical hacking plays a vital role in maintaining and saving a lot of secret information, whereas malicious hacking can destroy everything. What all depends is the intension of the hacker. It is almost impossible to fill a gap between ethical and malicious hacking as human mind cannot be conquered, but security measures can be tightening.

REFERENCES

[1] Wikipedia.
[2] Bhawana Sahare, Ankit Naik, Shashikala Khandey, Department of Computer Science and Engineering, Kirodimal Institute of Technology, Raigarh Chhattisgarh, India.
[3] V.Chandrika, Department of Computer Science, KBN College, Vijayawada, Andhra Pradesh, India.
[4] Ethical hacker Anand Prakash
http://www.cxotoday.com/story/india-is-in-desperate-need-for-an-army-of-ethical-hackers.