Ethical Hacking

Stuti Tandon, Anshika Saxena, Vaibhav Srivastav
College of Computing science and technology

Abstract- In today's world where the information communication technique has brought the world together there is one of the increase growing areas is security of network ,which certainly generate discussion of ETHICAL HACKING . The main reason behind the discussion of ethical hacking is insecurity of the network i.e. hacking. The need of ethical hacking is to protect the system from the damage caused by the hackers. The main reason behind the study of ethical hacking is to evaluate target system security & report back to owner. This paper helps to generate a brief idea of ethical hacking & all its aspects.

Index Terms- Hacker, security, firewall, automated, hacked, crackers

I. INTRODUCTION OF HACKING

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. To better describe hacking, one needs to first understand hackers. One can easily assume them to be intelligent and highly skilled in computers. In fact, breaking a security system requires more intelligence and expertise than actually creating one. To counter attack them ethical hacker's are used in the Govt. organization, companies etc. A hacker is a term that first started being used in the 1960s and described a programmer or someone who hacked computer code. Later the term evolved into an individual who had an advanced understanding of computers, networking, programming, or hardware, but did not have any malicious intents.

Today the hacker is the most important player for governments and cyber warfare but not only, private companies and industry of crime consider him as the repository of knowledge that has become crucial, the mastery of new technology.

IV. FATHER OF HACKING

In 1981, Ian Murphy, also known as "Captain Zap", became the first hacker to be convicted of hacking. He hacked into the AT&T computer network and modified the billing rates system, changing the internal clocks so that cheaper late-night rates were billed to customers during mid-day hours.

V. TOOLS OF HACKING

Pentesting software hacker tools as used by hackers, geeks, ethical hackers and security engineers. These tools are opensource.

- Nmap
- Metaspoilt Penetraition Testing Software
- John The Ripper
- THC Hydra
- OWASP Zed
- Wireshark
- Maltego
- Cain and Abel
- Beef
- Nikto

II. TECHNIQUES OF HACKING

Some of the hacking techniques that are commonly used

- Bait and switch
- Cookie theft
- Clickjacking attack
- Virus, Trojan etc.
- Phishing
- Evesdropping
- Fake WAP
- Deniel of Service
- Keylogger

III. NEED OF HACKING

Hacking is very important practice in the modern day society because hacker's are the experts in how the system functions and how the system can fail.

VI. ROLE OF HACKERS

An ethical hacker uses port scanning tools like Nmap, Nessus to scan one's own systems and find open ports. The vulnerabilities with each of the ports can be studied and remedial measures can be taken.
A ethical hacker will examine patch installations and make sure that they cannot be exploited.
An ethical hacker will see if he/she can evade IDS (Intrusion Detection systems), IPS (Intrusion Prevention systems), honeypots and firewalls. In addition to this, an ethical hacker can employ other strategies like sniffing networks, bypassing and cracking wireless encryption, and hijacking web servers and web applications.
Sniffing networks, bypassing and cracking wireless encryption, and hijacking web servers and web applications.
Ethical hackers may also handle issues related to laptop theft and employee fraud.

VII. FEATURES OF ETHICAL HACKING

----- E.H. has some distinct features which when compared to security and problem scanning.
-----It is highly or completely automated.

----- E.H. typically exploits the security in order to access the data or access another system.

It provides security to the system and network.

----- It helps to exposes the true risk causing to the system or network.

VIII. ETHICAL HACKING PROCESS

Ethical hacking needs advance planning strategic and tactical issues in the ethical hacking process should be determined , planning is important for testing.

For example: - from a simple password cracking to all out penetration test on a web application. Approval of plan for ethical hacking is essential for the process of hacking.

Sponsorship of the project is the most important step for ethical hacking process because one needs someone to protect the plan , otherwise testing can be unexpectedly called off.

A well define plan includes the following information:-

----- System to be tested

----- Risks that are involved

----- When the tests are performed and your overall timeline

-----how the tests are performed

-----how much knowledge of the systems you have before you start testing

-----what is done when a major threat is discovered.

IX. USE OF TOOLS FOR ETHICAL HACKING

Ethical hacker needs to understand how to find the network range and subnet mask of the target system. IP addresses are used to locate, scan and connect the target systems. Ethical hacker also should find out the geographical location of target system. This can be done by tracing the messages that are sent to destination and the tools used are traceroute, Visual route and NeoTrace to identify the route the target (Kimberly Graves, 2007). Ethical hacking should use right tools or else task accomplishment of task effectively is difficult. Many security assessment tools will produce false positive and negative or may they even miss susceptibility to attacks. In case of tests in case of physical security assessments they miss weakness. In order for ethical hacking specific tools have to be used for the task chosen. The easier the ethical hacking will become if many tools are used. The right tool must be used at right place. The characteristics in tools for ethical hacking is it should have sufficient document, detailed reports should be there on the discovered attacks regarding their fixing and explosion, Updates and support. The general tools used for ethical hacking in case to find passwords are cracking tools such as LC4, John the Ripper and pwdump (Bragg, Mark Phodes Ouslev and Keith Strassberg, 2004). The general tools like port scanner like SuperScan cannot be used to crack passwords. The Web-assessment tools such as Whisker or WebInspect tools are used for analysis of Web applications in depth. Whereas network analyzer tools such as ethereal cannot give good results. While using the tools for any particular task it is better to get feedback from the simple Google searches such as SecurityFocus.com, SearchSecurity.com and Itsecurity.com will give nice feedback from the other security experts which makes ethical hacking easy and to select the right tool. Some of the commercial, freeware and open source security tools are Nmap (Network Mapper), Etherpeek, SuperScan, QualysGuard, WebInspect and LC4, LANguard Network Security Scanner, Network Stumbler and ToneLoc. The capabilities of many security and hacking tools are often misunderstood, such as SATAN (Security Administrator Tool for Analyzing Networks) and Nmap. The other popular tools used in ethical hacking are Internet scanner, Ethreal, Nessus, Nikto, Kismet and THC-Scan (Kevin Beaver, 2007). Cain and able is a ethical tool used for recovery of windows UNIX problems. This is only password recovery tool handles an enormous variety of tasks. It can recover the password by sniffing the network, cracking the encrypted passwords using Dictionary and Cryptanalysis, recording VoIP conversations, decoding scrambled passwords, revealing the password boxes, uncovering cached passwords and analyzing routing protocols. Ethereal is a fantastic open source tool used as network protocol for UNIX and Windows. It allows examining the data which is present in disk or file and can capture the data. This is also known as Wire shark. It has many powerful features which have very rich display filter language and ability to view the TCP session. Another cracking tool Aircrack is the fastest available cracking tool (John Hyuk Park, Hsiao-Hwa Chen and Mohammed Atiquzzaman, 2009). Thus proper tools and techniques has to be used for better hacking and it will be easier by using more and more tools required.

- FACTS ABOUT ETHICAL HACKING

1. India leads the world in ethical hackers; 23% live there (the U.S. is number two with 20%).
2. Top ethical hackers in India make 16 times the median salary for a software engineer in that country
3. 58% call themselves "self-taught," but many report they've taken at least some computer science classes
4. Top motivations are "the opportunity to learn tips and techniques," “to be challenged, and “to have fun”; "making money" was 4th
5. 37% hack as a hobby
6. 12% make more than $20,000 annually
7. 3% make more than $100,000 annually
8. 1% make more than $350,000 annually
9. Young person's game: 90% of hackers are younger than 35

X. TERMS RELATED TO HACKING

- SQL INJECTION

SQL injection is a code injection technique that might destroy your database.

SQL injection is one of the most common web hacking techniques.

SQL injection is the placement of malicious code in SQL statements, via web page input.

- KEYLOGGER

A keylogger (short for keystroke logger) is software that tracks or logs the keys struck on your keyboard, typically in a covert manner so that you don't know that your actions are being monitored. This is usually done with malicious intent to collect your account information, credit card numbers, user names, passwords, and other private data.

- CROSS SITE SCRITING(XSS)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts (also commonly referred to as a malicious payload) into a legitimate website or web application. XSS is amongst the most rampant of web application vulnerabilities and occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

By leveraging XSS, an attacker does not target a victim directly. Instead, an attacker would exploit a vulnerability within a website or web application that the victim would visit, essentially using the vulnerable website as a vehicle to deliver a malicious script to the victim's browser.

While XSS can be taken advantage of within VBScript, ActiveX and Flash (although now considered legacy or even obsolete), unquestionably, the most widely abused is JavaScript – primarily because JavaScript is fundamental to most browsing experiences.

XI. HACKER GOOD, CRACKER BAD

A *hacker* is a person intensely interested in the arcane and recondite workings of any computer operating system. Hackers are most often programmers. As such, hackers obtain advanced knowledge of operating systems and programming languages. They might discover holes within systems and the reasons for such holes. Hackers constantly seek further knowledge, freely share what they have discovered, and never intentionally damage data.A lower form of crackers, script kiddies are not particularly knowledgeable about computer and networking details. Instead, they download ready-made tools to seek out weaknesses on systems accessible via the Internet. They do not target specific information or a specific company but rather scan for opportunities to disrupt and vandalize systems. Most "hackers" and "hacking" events reported on by the popular press are actually of this type. A cracker is someone who breaks into someone else's computer system, often on a network bypasses passwords or licenses in computer programs or in other ways intentionally breaches computer security. A cracker can be doing this for profit, maliciously, for some altruistic purpose or cause, or because the challenge is there. Some breaking-and-entering has been done ostensibly to point out weaknesses in a site's security system. Crackers or Black Hat hackers or cheaters or simply criminals, they are called criminals because they are having the mindset of causing harm to security and they steals very useful data and use it in wrong ways. Phishers also come in this category who steals account info and steal your credit card nos. and money over the Net.

REFERENCES

[1] Encyclopaedia Britannica. 2003. Encyclopaedia Britannica Premium Service. 28 Oct, 2003 <http://www.britannica.com/eb/article?eu=102011>.

[2] <https://en.wikipedia.org/wiki/Hacking_tool>.

[3] <https://www.w3schools.com/sql/sql_injection.asp