Academic Science

International Journal of Innovations & Advancement in Computer Science
IJIACS
ISSN 2347 – 8616
Volume 4, Special Issue
May 2015

Ethical Hacking: A Security Assessment Tool to Uncover Loopholes and Vulnerabilities in Network and to Ensure Protection to the System

Mr. Prakash Chandra Behera
Assistant Professor
Department of Sciences
St. Claret College
MES Ring Road
Jalahalli, Bangalore-560013

Mr. Chinmaya Dash
Assistant Professor
Department of Sciences
St. Claret College
MES Ring Road
Jalahalli, Bangaloe-560013

Abstract:
During the development of the Internet, computer security has become a major concern for different industries, businesses and Governments. The organizations use the Internet for electronic commerce, advertising, information distribution and access, and other pursuits, but they are worried about the possibility of being "hacked". Ethical Hacking increases security protection. Public and Private organizations migrate more of their critical information through 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 with good intentions. This paper describes what ethical hacking is, what it can do, methods & modes of ethical hacking, types of ethical hacking, different tools used for ethical hacking and concept of system security.

Keywords: Vulnerabilities, Hacker, mode of hacking, types and tools of hacking and System Security

INTRODUCTION

The vast growth of Internet has brought many technological advances like electronic commerce, email, easy access to vast stores of reference material etc .In the other side the hackers secretly steal the organization's information and transmit it to the open internet. These types of criminal hackers are called black hat hackers. So, to overcome these major issues, another category of hackers came into existence and these hackers are termed as ethical hackers or white hat hackers. This paper describes 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 focused 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. 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

International Journal of Innovations & Advancement in Computer Science
IJIACS
ISSN 2347 – 8616
Volume 4, Special Issue
May 2015

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.

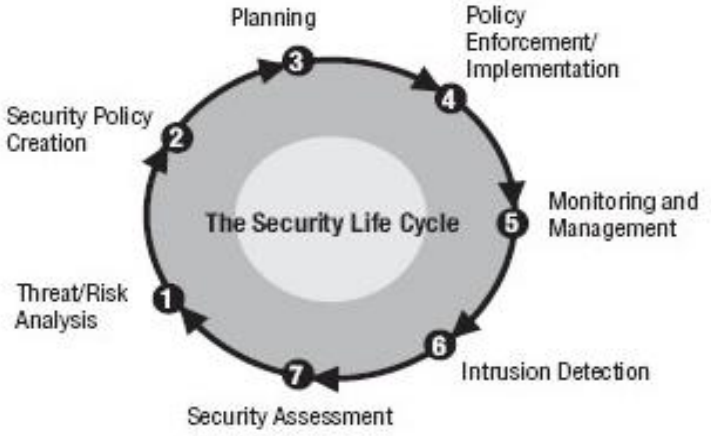

Fig 1: Security Life Cycle

Morals of an Ethical Hacker:

1. Obeying the Ethical Hacking Commandments: Every Ethical Hacker must follow few basic principles. Most of the time these principles get ignored or forgotten while planning or executing ethical hacking tests. The test results are even very dangerous.

2. Working ethically: The word ethical can be defined as working with high professional morals and principles. Whether you're performing ethical hacking tests against your own systems or for someone who has hired you, everything you do as an ethical Hacker must be approved and must support the company's goals. The misuse of information is absolutely not allowed.

3. Respecting privacy: Ethical Hacker must treat the information with complete respect. The passwords pertaining to these information must be kept private.

4. Not crashing your own systems: One of the biggest mistakes is when people try to hack their own systems; they come up with crashing their systems. The main reason for this is poor planning. These testers have not read the documentation or misunderstand the usage and power of the security tools and techniques. You can easily create miserable conditions on your systems when testing. Running too many tests too quickly on a system causes many system lockups. Many security assessment tools can control how many tests are performed on a system at the same time. These tools are especially handy if you need to run the tests on production systems during regular business hours.

5. Executing the plan: In Ethical hacking, time and patience are important. One must be very careful while performing the ethical hacking tests.

TYPES OF HACKER

White Hat Hackers: White hat hackers are ethical hackers with some certifications such as CEH (Certified Ethical Hacker). They break into systems just for legal purposes. Their main motive is to find loopholes in the networks and rectifying them. These type of hackers work with famous companies in securing their systems and protecting them against other hackers.

Black Hat Hacker: A black hat hacker may or may not have any hacking certification but they hold good knowledge about hacking. They use their skills for destructive purposes. They break into systems and networks either for fun or to gain some money by illegal means. They gain unauthorized access and destroy/steal confidential data and cause problems to their target.

Gray Hat Hacker: A grey hat hacker is a combination of a Black Hat and a White Hat Hacker. A Grey Hat Hacker may surf the internet and hack into a computer system for the sole purpose of notifying the administrator that their system has been hacked. They may offer to repair their system for a small fee.

MODE OF ETHICAL HACKING:

Insider attack: This ethical hack simulates the types of attacks and activities that could be carried out by an authorized individual with a legitimate connection to the organization's network.

Outsider attack :This ethical hack seeks to simulate the types of attacks that could be launched across the Internet. It could target Hypertext Transfer Protocol, Simple Mail Transfer Protocol (SMTP), Structured Query Language, or any other available services.

Stolen equipment attack: This simulation is closely related to a physical attack as it targets the organization's equipment. It could seek to target the CEO's laptop or the organization's backup tapes. No matter what the target, the goal is to extract critical information, usernames, and passwords.

Physical entry: This simulation seeks to test the organization's physical controls. Systems such as doors, gates, locks, guards, closed circuit television (CCTV), and alarms are tested to see whether they can be bypassed.

Bypassed authentication attack: This simulation is tasked with looking for wireless access points (WAP) and modems. The goal is to see whether these systems are secure and offer sufficient authentication controls. If the controls can be bypassed, the ethical hacker might probe to see what level of system control can be obtained.

Social engineering attack: This simulation does not target technical systems or physical access. Social engineering attacks target the organization's employees and seek to manipulate them to gain privileged information. Proper controls, policies, and procedures can go a long way in defeating this form of attack.

STEPS INVOLVED IN HACKING PROCESS

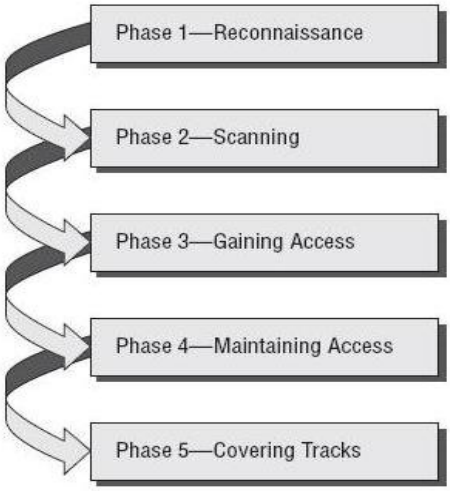

Fig 2: Process of Hacking

1. **Reconnaissance:** To be able to attack a system systematically, a hacker has to know as much as possible about the target. It is important to get an overview of the network and the used systems. Information such as DNS servers, administrator contacts and IP ranges can be collected. During the

reconnaissance phase different types of tools can be used – network mapping, network and vulnerability scanning tools are commonly used. Cheops for example is a very good network mapping tool generates networking graphs. These maps gives an overview about the network and helps during the attack phase. A network mapping tool is very helpful when doing an internal ethical hack. At the end of the reconnaissance phase, an attacker should have a bunch of information about the target. With all these pieces of information, a promising attack path can be constructed.

2. **Probe and Attack**: This is a phase 2 process as shown in the above fig. The probe and attack phase is about digging in, going closer and getting a feeling for the target. It's time to try the collected, possible vulnerabilities from the reconnaissance phase. Tools which can be used during the Probe and Attack phase are many-sided as web exploits; buffer overflows as well as brute-force can be applied. Even Trojans like Net Bus can be deployed to capture keystrokes, get screenshots or start applications and a host. The probe and attack phase becomes very time consuming, especially if brute force attack techniques are used or when individual pieces of software needs to be developed or analyzed.

3. **Listening:** This is again a phase 2 process i.e. scanning which is a combination of Probe and attack and listening. Listening to network traffic or to application data can sometimes help to attack a system or to advance deeper into a corporate network. Sniffers are heavily used during the listening phase. Sniffers can be simple or complex in nature. It can be console based or GUI driven.

4**. First Access**: This is a phase 3 process which is not about getting root access, it's about getting any access to a system be it a user or root account. Once this option is available it's time to go for higher access levels or new systems which are reachable through the acquired system.

5. **Advancement**: Phase 4 i.e. Maintaining access is a combination of Advancement and Stealth process. The advancement phase is probably the most creative demanding stage, as unlimited possibilities are open. Sniffing network traffic may unveil certain passwords, needed usernames or e-mail traffic with usable information. Sending mails to administrators faking some known users may help in getting desired information or even access to a new system. Last but not least, installing new tools and helpful scripts may help to dig in deeper or to scan log files for more details.

6. **Stealth:** Some systems may be of high value – systems which act as routers or firewalls, systems where a root account could be acquired. To have access to such systems at a later time it is important to clean relevant log files.

7. **Takeover:** Takeover is a phase 5 process. Once root access could be attained, the system can be considered won. From there on it's possible to install any tools, do every action and start every services on that particular machine. Depending on the machine it can now be possible to misuse trust relationships, create new relationships or disable certain security checks.

8. **Cleanup:** This could be instructions in the final report on how to remove certain Trojans but most of the time this will be done by the hacker itself. Removing all traces as far as possible is kind of a duty for the hacking craft.

An ethical hack always poses a certain risks if not properly done. A hacker could use the deployed tools or hide his attacks. He could also try to attack the attackers system, therefore gain entry to the ethical hackers system and collect all information free of charge, sorted and prepared. Preparing an ethical hack and hold a high level of security is a challenging task which should only be done by professionals.

TOOLS USED IN ETHICAL HACKING

It is very much essential to make sure that we are using the right tool for ethical hacking process. It is important to know the personal as well as technical limitations. Many tools focus on specific tests, but no one tool can test for everything. For example, to crack passwords (you need a cracking tools

such as LC4 or John the Ripper are needed. Similarly, for an in-depth analysis of a Web application, a Web-application assessment tool is more appropriate than a network analyser (such as Ethereal).
There are various characteristics for the use of tools for ethical hacking which are as follows:
1. Adequate documentation
2. Detailed reports on the discovered vulnerabilities, including how they can be fixed
3. Updates and support when needed
4. High level reports that can be presented to managers
These features can save the time and effort when we are writing the report. Time and patience are important in ethical hacking process. One should be careful when performing the ethical hacking tests. It is not practical to make sure that no hackers are on our system. It is good to keep everything private if possible. Do encrypt the emails and files if possible. The list and description of various tools used in the ethical hacking process are as follows:

1. **Scanning tools**: The Scanning tools are quite helpful in the ethical hacking process. In technical detail, a scanner sends a message requesting to open a connection with a computer on a particular port. (A port is an interface where different layers of software exchanges information). The computer has various options like - ignoring the message, responding negatively to the message, or opening a session. Ignoring the message is the safest since if there are no open services it may be hard for a cracker to determine if a computer exists. Once a port scan reveals the existence of an open service, a cracker can attack known vulnerabilities. Once a cracker scans all computers on a network and creates a network map showing which computers are running on which operating systems and what services are available, almost any kind of attack is possible including automated scripting program attacks and social engineered attacks. The first scanner was the security administrator's tool for analysing networks SATAN introduced by Dan Farmer in 1995. SATAN (Security Administrator tool for analysing networks) could analyse any system accessible over the internet. But the question here is that why should anyone with internet presence and no interest in cracking other systems learn about scanners? The answer is to learn what crackers will see in their own internet presence since scanners are common attack starting points. Crackers look for unauthorized services such as someone running a server with known problems, an unauthorized server on a high port etc. Port scanning can be done manually from a single computer to learn about target systems or it can be done automatically by program originating from multiple computers on different networks to a single target system over a long period of time. Port scanners like other tools, have both offensive and defensive applications- what makes a port scanner good or evil. Actually, a port scanner is simultaneously both the most powerful tool an ethical hacker can use in protecting the network of computers and the most powerful tool a cracker can use to generate attacks.

Commercial scanners	Network Assoc- Cybercop
Sniffers	Ethercap, tcpdump
Network scanners	SATAN, strobe, rprobe
War- dialing	ThcScan, LoginH
Password crackers	John the Ripper, L0pth crack
Firewall scanners	Firewalk
Security and vulnerability scanning	Nessus, ISS, cybercop

Table 1: Scanning Tools

2. Password cracking tools: Password cracking does not have to involve fancy tools, but it is a tedious process. If the target doesn't lock you out after a specific number of tries, you can spend an infinite amount of time trying every combination of alphanumeric characters. It's just a question of

time and bandwidth before you break into a system. There are three basic types of password cracking tests that can be automated with tools:

Dictionary- A file of words is run against user accounts, and if the password is a simple word, it can be found pretty quickly.

Hybrid: A common method utilized by users to change passwords is to add a number or symbol to the end.A hybrid attack works like a dictionary attack, but adds simple numbers or symbols to the password attempt.

Brute force: The most time consuming, but comprehensive way to crack a password. Every combination of character is tried until the password is broken.

Brutus	It is a password cracking tool that can perform both dictionary attacks and brute force attacks where passwords are randomly generated from a given character. Brutus can crack the multiple authentication types, HTTP (Basic authentication, HTML Form/CGI), POP3, FTP, SMB and Telnet.
Web cracker	It is a simple tool that takes text lists of usernames and passwords, and uses them as dictionaries to implement basic authentication password guessing.
ObiWan	It is a Web password cracking tool that can work through a proxy. ObiWan uses wordlists and alternations of numeric or alpha-numeric characters as possible passwords.

Table 2: Web password cracking tool

3. Port Scanning tools: Port scanning is one of the most common reconnaissance techniques used by testers to discover the vulnerabilities in the services listening at well-known ports. Once you've identified the IP address of a target system through foot printing, you can begin the process of port scanning: looking for holes in the system through which you -- or a malicious intruder -- can gain access. A typical system has 2^16 -1 port numbers, each with its own TCP and UDP port that can be used to gain access if unprotected. The most popular port scanner for Linux, Nmap, is also available for Windows. Nmap can scan a system in variety of stealth modes, depending upon how undetectable you want to be. Nmap can determine a lot of information about a target, like which hosts are available, what services are offered and which OS is running.

4. Vulnerability scanning tools: A Vulnerability scanner allows you to connect to a target system and check for such vulnerabilities as configuration errors. A popular vulnerability scanner is the freely available open source tool Nessus. Nessus is an extremely powerful scanner that can be configured to run a variety of scans. While a windows graphical front end is available, the core Nessus product requires Linux to run. Microsoft's Baseline Security Analyser is a free Windows vulnerability scanner. MBSA can be used to detect security configuration errors on local computers or remotely across a network. Popular commercial vulnerability scanners include Retina Network Security Scanner, which runs on Windows, and SAINT, which runs on various Unix/Linux versions.

ADVANTAGES OF ETHICAL HACKING:

Ethical hacking nowadays is backbone of network security. Each day its relevance is increasing.

1. To catch a thief you have to think like a thief.
2. Helps in closing the open holes in the network.
3. Provides security to banking and financial organization.
4. Prevents website defacements.
5. An evolving technique

International Journal of Innovations & Advancement in Computer Science
IJIACS
ISSN 2347 – 8616
Volume 4, Special Issue
May 2015

SYSTEM SECURITY

System security means securing a system from unauthorized access. Broadly we can divide security in three divisions

1. System security
2. Data Security
3. Network Security

System security is further divided into two divisions

1. Data accessible restriction
2. System accessible restriction

1. Data accessible restriction: -Data accessible security by many ways. Some the ways are
   - Encrypting Hard disk
   - Hiding Folders
   - By locking folders

2. System Accessible restriction: - System accessible restriction means restricting someone to access the system completely it can be referred as OS level security. The easiest way is to provide user password in the system.

TIPS FOR SECURING DATA AND SYSTEM

1. Install and Use Anti-Virus, firewalls & Anit key logger Programs
2. While installing OS like Windows XP give admin password.
3. Use Care When Reading Email with Attachments and following links.
4. Install and Use a Firewall Program
5. Make Backups of Important Files and Folders
6. Use Strong Passwords and change it regularly as you change your toothbrush.
7. Use Care When Downloading and Installing Programs
8. Install and Use a Hardware Firewall
9. Install and Use a File Encryption Program and Access Controls
10. Safeguard your Data
11. Real-World Warnings keep you safe online.
12. Keeping Children Safe Online
13. Use SYSKEY for password protection.

CONCLUSION

This paper addressed ethical hacking from several perspectives. Ethical hacking seems to be a new buzz word although the techniques and ideas of testing security by attacking an installation aren't new at all. But, with the present poor security on the internet, ethical hacking may be the most effective way to plug security holes and prevent intrusions.

On the other hand ethical hacking tools have also been notorious tools for crackers. So, at present the tactical objective is to stay one step ahead of the crackers. 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. After all, ethical hacking will play a certain role in the security assessment offerings and certainly has earned its place among other security assessments. In conclusion, it must be said that the ethical hacker is an educator who seeks to enlighten not only the customer, but also the security industry as a whole. In an effort to accomplish this, let us welcome the Ethical Hacker into our ranks as a partner in this quest.

REFERENCES

[1] H.M David, "Three Different Shades of Ethical Hacking: Black, White and Gray," in GSEC Practical Assignment, Version 1.4b, Option 1,Feb 23, 2004.
[2] Sanctum Inc, "Ethical Hacking techniques to audit and secure web enabled applications", 2002.
[3] Smith B., Yurcik W., Doss D., "Ethical Hacking: the security justification redux", IEEE Transactions, pp. 375-379, 2002.
[4] B. Reto, "Ethical Hacking", in GSEC Practical Assignment, Version 1.4b, Option 1, Nov 24, 2002.
[5] B. Kevin, "Hacking for dummies", 2nd edition, 408 pages, Oct 2006.
[6] D. Manthan "Hacking for beginners", 254 pages, 2010.
[7] my.safaribooksonline.com/.../introduction-to-ethical-hacking-ethics-legality.
[8] J. Danish and A. N. Muhammad, "Is Ethical Hacking Ethical? " , International journal of Engineering Science and Technology, Vol 3 No. 5,pp. 3758-3763, May 2011.
[9] Ajinkya A. Farsole, Amurta G. Kashikar and Apurva Zunzunwala , "Ethical Hacking ", International journal of Computer Applications (0975-8887), Vol. 1 No. 10, pp. 14-20, 2010.
[10] media.techtarget.com/searchNetworking- Introduction to ethical hacking-Tech Target