International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 11 Issue 4 –NOVEMBER 2014.

A Technique to Enhance Information Security in Ethical Hacking

KAVURI SRIDHAR

Head, Department of Computer Science, P.B. Siddhartha College of Arts & Science, Vijayawada

Abstract— The condition of security on the web is awful and deteriorating. One response to this condition of undertakings is termed as Ethical Hacking which endeavours to build security insurance by distinguishing and fixing known security vulnerabilities on frameworks possessed by different gatherings. As open and private associations move a greater amount of their basic capacities to the Internet, lawbreakers have more open door and motivation to get access to delicate data through the Web application. Along these lines the need of securing the frameworks from the annoyance of hacking produced by the programmers is to advance the persons who will punch back the illicit assaults on our machine frameworks. Thus, Ethical hacking is an appraisal to test and check a data innovation environment for conceivable frail connections and vulnerabilities. Moral hacking depicts the procedure of hacking a system in a moral route, hence with great plans. This paper depicts what moral hacking is, the thing that it can do, a moral hacking approach and in addition a few devices which can be utilized for a moral hack.

Keywords: Vulnerabilities, Hacker, Cracker, Port and Intrusion.

I. INTRODUCTION

The inconceivable development of Internet has brought a lot of people great things like electronic trade, email, simple access to endless stores of reference material and so forth. As, with most mechanical advances, there is likewise other side: criminal programmers who will furtively take the association's data and transmit it to the open web. These sorts of programmers are called dark cap programmers. Along these lines, to overcome from these significant issues, an alternate class of programmers started to be and these programmers are termed as moral programmers or white cap programmers. In this way, this paper portrays moral programmers, their aptitudes and how they go about helping their clients and attachment up security gaps. Moral programmers perform the hacks as security tests for their frameworks. This kind of hacking is constantly lawful and dependable. In different terms moral hacking is the trying of assets for the improvement of engineering and is focused on securing and ensuring IP frameworks. In this way, if there should be an occurrence of machine security, these tiger groups or moral programmers would utilize the same traps and methods that programmer utilize yet as a part of a lawful way and they would not one or the other harm the neither target systems nor take data. Rather, they would assess the focus on framework's security and report once again to the managers with the vulnerabilities they discovered and directions for how to cure them. Moral hacking is a method for doing a security evaluation. Like all other appraisals a moral hack is an irregular specimen and passing a moral hack doesn't mean there are no security issues. A moral hack's results is a definite report of the discoveries and additionally a confirmation that a programmer with a certain measure of time and aptitudes is or isn't ready to effectively assault a framework or get access to certain data. Moral hacking can be arranged as an issue evaluation, a sort of preparing, a test for the security of a data engineering environment. A moral hack demonstrates the dangers a data engineering environment is confronting and activities can be gone for broke or to acknowledge them.

We can easily say that Ethical hacking does perfectly fit into the security life cycle shown in the below figure,

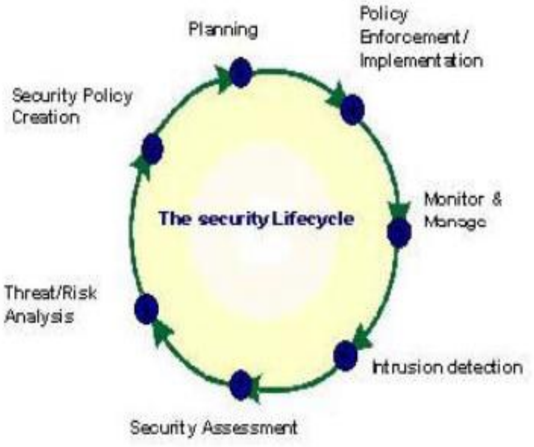

Fig. 1 Security life cycle

II. WORKING OF AN ETHICAL HACKER

The working of an ethical hacker involves the under mentioned steps:

1. Obeying the Ethical Hacking Commandments: Every Ethical Hacker must follow few basic principles. If he does not follow, bad things can happen. Most of the time these principles get ignored or forgotten when planning or executing ethical hacking tests. The 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. No hidden agendas are allowed. Trustworthiness is the ultimate objective. The misuse of information is absolutely not allowed.

3. Respecting Privacy: Treat the information you gather with complete respect. All information you obtain during your testing from Web application log files to clear-text passwords must be kept private.

4. Not crashing your 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. Be careful when you're performing your ethical hacking tests.

III. ETHICAL HACKING PROCESS

The Ethical hacking process needs to be arranged ahead of time. All specialized, administration and strategically issues must be considered. Arranging is critical for any measure of testing from a basic watchword test to full scale entrance test on a web application. Reinforcement off information must be guaranteed, overall the testing may be canceled startlingly on the off chance that somebody asserts they never approves for the tests. Thus, a decently characterized extension includes the accompanying data:

1. Specific systems to be tested.

2. Risks that are involved.

3. Preparing schedule to carry test and overall timeline. Gather and explore knowledge of the systems we have before testing. What is done when a major vulnerability is discovered?

4. The specific deliverables- this includes security assessment reports and a higher level report outlining the general vulnerabilities to be addressed, along with counter measures that should be implemented when selecting systems to test, start with the most critical or vulnerable systems.

The overall hacking methodology consists of certain steps which are as follows:

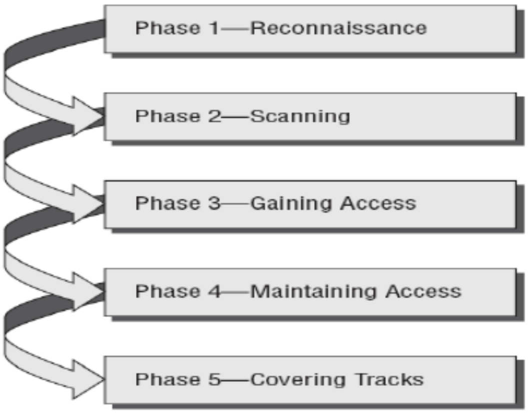

Fig.2 Phases of hacking.

1. Reconnaissance: To have the capacity to assault a framework efficiently, a programmer needs to know however much as could reasonably be expected about the target. It is vital to get a diagram of the system and the utilized frameworks. Data as DNS servers, chairman contacts and IP extents can be gathered. Amid the observation stage distinctive sort of apparatuses can be utilized – system mapping, system and helplessness examining instruments are the normally utilized. Cheops for instance is a decent system mapping instrument which has the capacity create systems administration charts. They can be of extraordinary help later on amid the assault stage or to get a review about the system. A system mapping instrument is exceptionally useful while doing an inner moral hack. Toward the end of the observation stage, an aggressor ought to have a bundle of data about the target. With all these bits of data, a guaranteeing assault way can be constructed.

2. Probe and Attack: This is a stage 2 procedure as indicated in the above fig. The test and assault stage is about diving in, going closer and getting an inclination for the target. Now is the right time to attempt the gathered, conceivable vulnerabilities from the observation stage. Devices which can be utilized amid the Probe and Attack stage are versatile as web endeavors; cradle floods and also savage energy can be needed. Indeed Trojans like NetBus can be sent to catch keystrokes, get screenshots or begin applications and a host. The test and assault stage can be extremely drawn out, particularly if animal power assault systems are utilized or 3. Listening: This is again a stage 2 procedures i.e. checking which a mix of Probe and assault is and tuning in. Listening to system movement or to application information can off and on again help to assault a framework or to development deeper into a corporate system. Listening is particularly capable when one has control of an essential correspondence bottleneck. Sniffers are vigorously utilized amid the listening stage.

Different sniffers, from extremely easy to more buildings, from support based to GUI driven exist for all working frameworks. A few sniffers, in the same way as ettercap can even toxin ARP tables to empower sniffing in exchanged situations and open completely new open doors for listening to system activity.

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 now reachable through the acquired system.

5. Advancement: Stage 4 i.e. Keeping up access is a mix of Advancement and Stealth process. The progression stage is most likely the most innovative requesting stage, as boundless conceivable outcomes are open. Sniffing system movement may uncover certain passwords, required usernames or email activity with usable data. Sending sends to overseers faking some known clients may help in getting craved data or even get to another framework. Likely one likewise needs to adjust design documents to empower or handicap administrations or gimmicks. To wrap things up, putting in new instruments and accommodating scripts may help to delve in deeper or to sweep log documents for more subtle elements.

6. Stealth: A few systems may be of high esteem- system which go about as switches or firewalls, frameworks where a root record could be gained. To have entry to such frameworks at a later time it is imperative clean pertinent log documents. Takeover: Takeover is a stage 5 methodology .Once root access could be accomplished; the framework can be viewed as won. From that point on it's conceivable to introduce any instruments, do each activity and begin each administration on that specific machine. Contingent upon the machine it can now be conceivable to abuse trust connections, make new connections or incapacitate certain security checks.

7. Cleanup: This could be directions in the last provide details regarding how to evacuate certain Trojans however more often than not this will be carried out by the programmer itself. Uprooting all follows the extent that this would be possible is slightly an obligation for the hacking art. A moral hack dependably represents a certain dangers if not appropriately done. A programmer could utilize the conveyed instruments or conceal his assaults in all the assaults from the moral hack. He could likewise attempt to assault the aggressors framework, thusly pick up passage to the moral programmers framework and gather all data complimentary and as of now sorted and arranged. Setting up a moral hack and hold an abnormal state of security is a testing assignment which ought to just be carried out by professionals.

IV. SELECTION OF TOOLS IN ETHICAL HACKING

It is all that much crucial to verify that we are utilizing the right instrument for moral hacking methodology. It is critical to know the individual and also specialized constraints. Numerous apparatuses concentrate on particular tests, however nobody apparatus can test for everything. The more instruments you have, the less demanding your moral hacking endeavors are. Verify you that you're utilizing the right device for the errand. Case in point, to break passwords, you require a breaking apparatus, for example, Lc4 or John the Ripper. So also, for an inside and out examination of a Web application, a Webapplication appraisal instrument, (for example, Whisker or Web inspect) is more suitable than a system analyzer, (for example, Ethereal). There are different attributes for the utilization of apparatuses for moral hacking which are as per the following:

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 gimmicks can spare the time and exertion when we are composing the report. Time and understanding are vital in moral hacking procedure. We ought to be cautious when we are performing the moral hacking tests. It is not reasonable to verify that no programmers are on our framework. Simply make a point to continue everything private if conceivable. Do scramble the messages and documents if conceivable. The rundown and depiction of different apparatuses utilized as a part of the moral hacking procedure are as per the following: 1. Scanning tools: The Scanning devices are truly useful in the ethical hacking procedure. In specialized point of interest, a scanner communicates something specific asking for to open an association with a machine on a specific port. (A port is an interface where distinctive layers of programming trades data). The machine has a choice of disregarding the message, reacting adversely to the message, or opening a session. Disregarding the message is the most secure since if there are no open administrations it might be hard for a wafer to figure out whether a machine exists. When a port sweep uncovers the presence of an open administration, a wafer can assault known vulnerabilities. When a wafer filters all machines on a system and makes a system guide demonstrating what machines are running, what working frameworks and what administrations are accessible, practically any sort of assault is conceivable including mechanized scripting project assaults and social designed assaults. The principal scanner was the security overseer's apparatus for dissecting systems – SATAN presented by Dan Farmer in 1995. SATAN (Security Administrator instrument for examining systems) could investigate any framework available over the web. Be that as it may the inquiry here is that why ought to anybody with web vicinity and no enthusiasm toward splitting different frameworks research scanners? The answer is to realize what saltines will see in their own particular web vicinity since scanners are basic assault beginning stages. Saltines search for unapproved administrations, for example, somebody running a server with known issues, an unapproved server on a high port. Port filtering is possible physically from a solitary machine to look into target frameworks or it is possible naturally by system starting from various machines on diverse systems to a solitary target system over a drawn out stretch of time. Port scanners like different instruments, have both hostile and preventive applications- what makes a port scanner great and shrewdness is the manner by which it is utilized. Really, a port scanner is all the while both the most compelling instrument a moral programmer can use in securing the system of machines and the most effective device a wafer can use to produce assaults. The table underneath demonstrates a portion of the checking devices that assistance in the ethical hacking process:

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

Fig.3 Tools of Ethical Hacking

2. Password cracking tools: Secret key splitting does not need to include extravagant instruments; however it is a dreary procedure. On the off chance that the target doesn't bolt you out after a particular number of tries, you can invest an interminable measure of time attempting each blend of alphanumeric characters. It's simply an inquiry of time and data transmission before you break into a system. There are three fundamental sorts of secret key splitting tests that can be robotized with instruments:

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

2. 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.

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

There are some common web passwords cracking tools which are as follows:

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.

3. Port Scanning tools: Port examining is a standout amongst the most well-known observation systems utilized by analyzers to find the vulnerabilities in the administrations listening at well-known ports. When you've recognized the IP location of a target framework through foot printing, you can start the procedure of port filtering: searching for gaps in the framework through which you - or a vindictive interloper - can get access. A common framework has 2^16 -1 port numbers, each with its own particular TCP and UDP port that can be utilized to get access if unprotected. The most prevalent port scanner for Linux, Nmap, is likewise accessible for Windows. Nmap can check a framework in mixed bag of stealth modes, contingent on how imperceptible you need to be. Nmap can focus a great deal of data around a focus, in the same way as what hosts are accessible, what administrations are offered and what OS is running.

4. Vulnerability scanning tools: A Vulnerability scanner permits you to associate with a target framework and check for such vulnerabilities as setup lapses. A famous defenselessness scanner is the openly accessible open source device Nessus. Nessus is a greatly compelling scanner that can be arranged to run a mixed bag of sweeps. While a windows graphical front end is accessible, the center Nessus item obliges Linux to run. Microsoft's Baseline Security Analyser is a free Windows powerlessness scanner. MBSA can be utilized to catch security arrangement slips on neighborhood machines or remotely over a system. Prominent business helplessness scanners incorporate Retina Network Security Scanner, which runs on Windows, and SAINT, which runs on different Unix/Linux forms.

V. CONCLUSION

This paper addressed ethical hacking from a few viewpoints. ethical hacking is by all accounts another trendy expression in spite of the fact that the procedures and thoughts of testing security by assaulting an establishment aren't new whatsoever. Anyway, with the present poor security on the web, ethical hacking may be the best approach to attachment security gaps and counteract interruptions. Then again ethical hacking instruments have likewise been famous apparatuses for saltines. In this way, at present the strategic target is to stay one stage in front of the wafers. ethical Hacking is an instrument, which if appropriately used, can demonstrate valuable for comprehension the shortcomings of a system and how they may be abused. After all, ethical hacking will assume a certain part in the security appraisal offerings and positively has earned its place among other security appraisals. Taking everything into account, it must be said that the moral programmer is a teacher who tries to edify the client, as well as the security business as an issue. In a push to fulfill this, let us respect the Ethical Hacker into our positions as an issue in this journey.

VI. REFFERENCES

[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 Ethical Hacking Ethical? " , International journal of Engineering Science and Technology, Vol 3 No. 5, pp. 3758-3763, May 2011.

[6] Ajinkya A. Farsole, Amurta G. Kashikar and ApurvaZunzunwala , "Ethical Hacking " , International journal of Computer Applications (0975-8887), Vol. 1 No. 10, pp. 14-20, 2010.

[7] media.techtarget.com/search Networking- Introduction to ethical hacking-Tech Target.