Ethical Hacking As A Method To Enhance Information Security.

Cyber attack protection methodology.

Nimesha Nishadhi
Department of Inter-Disciplinary Studies
Faculty of Information Technology
University of Moratuwa.
Katubedda, Sri Lanka
nnishadhi95@gmail.com

Abstract

In modern technical world internet is the main information provider and storing method. The security state on the internet is getting worse. Ethical Hacking techniques are introduced to increase online security by identifying known security vulnerabilities related with systems of others. The public and private organizations immigrate most of their crutial data to the internet, hackers and crackers have more opportunity to gain access to sensitive information through the online application. Therefore, the importance of securing the systems from the affliction of immense hacking is to encourage the persons who will caster back the illegal attacks on a computer system. Ethical hacking is an examination to check an information technology environment for potential exhausted links and vulnerabilities. Ethical hacking traverses the technique of hacking a network in an ethical manner including with virtuous viewpoint. This research paper explores ethical hacking introduction, types of ethical hackers, ethics behind ethical hacking, ethical hacking methodology, some tools which can be used for an ethical hack, cyber security concepts

Keywords-Hacker,Cracker,Ethicalhackers,Security,vulnarabilities

I. INTRODUCTION

The immense advancement of Internet has brought large amount of improvements like electronic commerce, email, easy access to giant depot of reference material, distance learning facilities, electronic banking. Calling to the disadvantages, the technical development, criminal hackers who will furtively steal the organization's or administrative data and information to transmit them to the open internet without privacy. This process is done by black hat hackers. The white hat hackers or Ethical hackers are another group of hackers who came into persistence to silence and overcome from the major issues done by black hat hackers. This research paper explains about ethical hackers, their skills, how ethical hackers helping their customers and plug up security holes and effects of cyber security. Ethical hackers conduct the hacking always legally and trustworthy manner as a security test for the systems. Therefore, ethical hacking raised as the testing of wealth for the technological betterment with focusing on s and protecting and securing IP systems. For the enhancement of Information security ethical hacker teams are applying the similar techniques and methodologies of a hacker but in a legal manner without harming the targeted systems or stealing the information. They evaluate the targeted system's security and report back to the owners with the vulnerabilities. They encountered and ordering with rectification instructions. Completing an ethical hack assessment through a system does not mean that the system is fully secured. An ethical hack's quotient is a well explained report based on the explorations and evidences. There by, a hacker consisting of certain amount of skills is or is not possible for the victoriously attack to a system and get access to kind of information. Ethical hacking can be classified as a security assessment, a way of practicing, an examination for security of an information technology background. The Ethical hack illustrate the risks that information technology background is confront of, and procedures that allows to minimize certain risks or to accept them. The following figure shows security life cycle which shows the Ethical hacking procedure ideally.

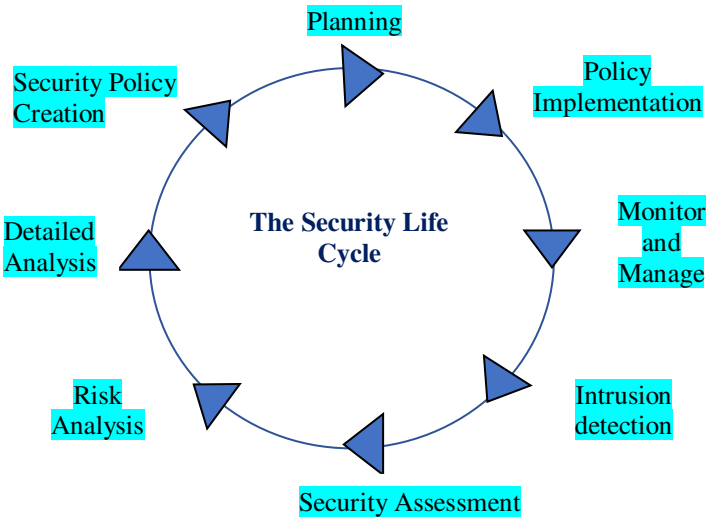


Figure 1

II. LITERATURE REVIEW

[4] Hacking can be explained as one of the misunderstood major cyber concepts. The greatest number of individuals think that hacking as something illegal or evil, but nothing can be farther from represented truth. It is clear that, hacking may be an actual threat, but to stop hacking yourself by someone , it is a must for you to learn hacking techniques.[3]Aman Gupta explained well about techniques and methods such as Wi-Fi hacking ,penetration testing and DOS attacks with the aim of providing a better knowledge in hacking methodologies and eventually preclude your devices or computer from being a target easily.[10] History of Computing carries all together up on to one minute coverage about all basic hacking concepts, issues and terminology , with all skills you have to keep developed in this field. The research thoroughly cover ups core hacking topics, such as assessments of vulnerabilities, virus attacks to the sites, hacking techniques, spyware and its activities, network defenses, passwords protection and detections, firewalls and its behavior, intrusion detection and VPN.[2] Ethical Hacking: The Security Justification Redux is a research with all extensively and clearly mentioned about art in both attacks and defense .

III.IDENTIFICATION ABOUT TYPES OF HACKERS

Hackers are malicious computer and technical experts in both software and hardware. He is a computer master and enthusiast in security, programming language and network knowledge. According to the manner of his performing and based on the individual intensions HACKERS can be classified as follows.

a. Black Hat Hackers
b. Grey Hat Hackers
c. White Hat Hackers

a. Black Hat Hackers

Black Hat Hackers also define as a “Cracker”. A cracker is a computer software and hardware expert brain who breaks into the security protection of other external person with having a malicious or bad desire or intentions to damage or steal their secret, curtail and important information. This is compromising the protection of the large organizations, closing down or functions altering of networks and websites. They exceed the security of the computer for their personal benefits. They are individuals who are generally needs to prove their comprehensive knowledge inside the computers and accomplish different types of cybercrimes like credit card fraud and identity stealing.

b. Grey Hat Hackers

Grey Hat Hackers are kind of computer hackers with knowledge on security expert sides who are sometimes violate the laws but they do not have intentions of any malicious activity. The word Grey Hat is formed from the White Hat and the Black Hat since the White Hat Hackers find and able to know the vulnerabilities inside the network ,computer system the networks and they do not reveal to any one else until the wrong is being fixed, on the other side the Black Hat Hackers illegally abuse the network or the computer system to search and identify vulnerabilities and inform other parties the way of doing such thing whereas the Grey Hat Hacker never ever illegally dispose or exploits to anybody else as such. The Grey Hat Hackers are stand in between the Black Hat Hackers who proceed malicious works to exploits the computer systems and White Hat Hackers who proceed with maintaining of a system in security protection.

3. White Hat Hackers

White Hat Hackers are possessed with specialist knowledge on computer security that breaks down into for the finding gaps in the fully secured networks and computer systems related to some of the organizations and companies. Then they work for correcting malicious actions by improving the protection or the security. The White Hat Hackers use their expert knowledge and experienced skills to protect the organization or the company before malicious are putting their hands on it and prevent the harm which is going to happen within the computer system or the network. Therefore, White Hat Hackers are type of authorized individuals in the industry, wherever the methods applied by both the party’s white hat and black hat hackers are similar and work with the permission from the company or the organization who hires them to proceed such.

IV. ETHICS TO FOLLOW IN ETHICAL HACKING

A. Conform with the Ethical Hacking Principles:

Every Ethical Hacker must follow and obey with a few basic principles to avoid from bad occurring. Most probably these principles get forgotten or ignored in planning or executing ethical hacking tests. This causes most dangerous results.

B. Operate in Ethical way:

As the word suggests ethical means working or proceeding with high professional principles and morals. In conducting ethical hacking tests for your own systems or for a person who has hired you, everything you perform as an Ethical Hacker must support the company’s goals and must be approved. Any kind of hidden agendas are not allowed. The ultimate objective is to ensure trustworthiness by un-allocating misuse of data and information.

C. Respecting towards the Privacy of the owners and information:

Behave with having a great respect towards the data and information you gather in the hacking process. The privacy of all the data and information which you gather during your testing from Web application log files to clear-text passwords must be protected.

D. Not crashing with your systems

When people try to hack other systems; they ended up with crashing their own systems is a significant mistake identified in this process. Poor planning is identified as the main reason in behind. Not reading the guidelines, not read the documentation or misunderstand the usage and power of the security tools and techniques by testers are few of the points identified as poor planning. It is easy to create miserable conditions on your systems when testing. Allowing to run many tests quickly on a system causes wide system lockups. Many security assessment tools can control number of tests are performed on a system at the parallel time periods. At the occasions which needs to proceed the tests on production systems during regular business hours these tools are capable enough.

E. The Plan Execution:

The most significant and most important attitudes of a hacker is time and patience bonded with skills towards the action launching. When performing ethical hacking procedures, it is better to be more careful.

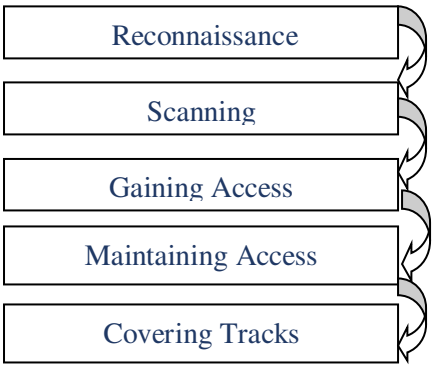
V. THE PROCESS OF ETHICAL HACKING

The advance type planning can be seen in Ethical hacking.

All kinds of technical, strategical and management issues should be considered. The proper planning is much more important for any kind of testing starting from a very simple and small password test to all the outer penetration tests on a web application or a web site. Backup offing data or information must be ensured. Since the testing might be break off unexpected way. If some person claims or suspended, they never authorize for the tests. Therefore, a well explained scope is involving with the following mentioned information.

a. What are the specific systems that should be tested?
b. What kind of Risks are involved?
c. Prepare a schedule to have test and overall based timeline.
d. Find out and explore the knowledge of systems that we are engage with before start testing.
e. The precautions to be done after a major vulnerability is exposed?
f. Clear outlet about the significant deliverables which includes the reports based on security assessment reports and the premium level reports about the popular vulnerabilities to be called.

VI. PHASES OF HACKING



First Phase: Reconnaissance

A hacker should have knowledge well about the hacking target to do an attack systematically for a system. It is noticeable to take an overview about the used systems and the network. Information transverse as DNS servers, the administrator contacts and IP address ranges are collected. Different kinds of tools are used in this phase like network, network mapping, and vulnerability scanning tools are most commonly used tools. As an example, Cheops can be mentioned. It is an excellent network mapping tool which can produce networking graphs. Those networking graphs are doing a big help on the upcoming attack phase and to have an network overview. To do a successful internal ethical hacking this tool is essential. The attacker must possess a bundle of information and data about the target at the end of this phase. A promising attack path is built up using this all information collected by reconnaissance phase.

Second Phase: Scanning

During the Scanning phase probe and attack are the two main processes that are proceed on. There by, excavate in, reaching to the closer and sensing a feeling to the target. Therefore, in this time, hacker must compete for the gathered, feasible vulnerabilities founded from the first phase (reconnaissance phase). Tools that are assigned to this phase are multi sided like web exploits. Buffer overflows and the brute force are required in this phase tool activating process. Here, Trojans like Net Bus able to deploy for capturing keystrokes, take screenshots and start applications and a host. This phase consumes very big time slot to complete. If brute force attack techniques are get used by hackers or when an individual petition of software to be improved and analyzed this phase is doing a massive work.

Listening is another second phase process. Probe, attack and listening are the main combinations of Scanning process. Having a listening to the network traffic or to having a listening to application data are instantly helpful to riposte a system for developing deep into a corporate or an associate network. Since the listening is more activate as soon as the one has limited with an essential bottleneck of communication. During the listening phase most, usable tools are Sniffers. These sniffers are built from simple to more complex forms as multiple sniffers. They are existing in all the operating systems as console based to GUI driven. Ettercap is a sniffer that can even poison ARP tables for enabling the sniffing action in switched surroundings. And, uncover totally new situations for network traffic listening.

Third Phase: Gaining Access

This is known as first access wherever this phase is not about the taking of root access only about taking any kind of access to the system, maybe it is a user account or root account. Since this access action is available with, this makes relevant time for going a premium access levels or newer systems which are currently reachable through the acquired system.

Fourth Phase: Maintaining access
This phase is an addition of stealth process and advancement. An advancement phase is presumably the vast creative demanding step, from all the unlimitedly opened possibilities. Sniffing network-traffic might uncover significant passwords, wanted usernames and traffic related to e-mail with the associated information. Sending e-mails to the administrators by faking the certain well-known users or clients might help in taking expected information, data or access to a fresh system. Probably, the person also must commute the configuration records to disable or enable features and services. At last installing of new tools to the devices and contributory scripts will helps to go in deep levels and to scan the logging records and files for descriptive details.
Stealth: Few systems are having higher valued systems which are acting as firewalls or routers, the systems, where there is having root account should be acquired. For the accessing to such kind of systems with a passed time, it is a must to clean and clear all the relevant logged records and files.

Fifth Phase: Takeover
Takeover is a process which, once the root access is arrived, the is considered as winner. Then after onwards it makes possible for installing any kind of tools, thereby it can perform each and every task and start each and every service upon the particular assigned machine. Based on the machine, now it is possible to wrongly access trust and worthy relationships, create new bondings or damage significant security checkups. Cleanup: This is an instruction set in a finalized report about the way of removing identified trojans. Even though of this is an action of the hacker itself. By removing and cleaning all the traces to the its greater extent is a way of duty for the hacking craft. In an ethical hack, it most occasions have a significant risk, only if the task could not properly complete. Therefore, a hacker is using all the dilated tools to hide its attacks from the attacks formed by the ethical hackers. Also, should try to attack for the attacker's system, as to take-up the entry for the system of ethical hackers and collection of all the information and data free of charge with an already prepared and sorted. Constructing an ethical hack scheme and holding a higher-level site security is a challengeable task that is became a duty of professionals.

VII. BENEFITS OF ETHICAL HACKING

Since ethical hacking engage with an excellent role model in modern security era, where the network using individuals are frequently increasing. The hacker types who gaining the advantages of network while staying at the home place. The following are the identified main advantages of ethical hacking.
a. The conflict against terrorism issues and security issues.
b. Preventing the action of malicious hackers to take the access of crucial data.
c. Ethical hackers think that an individual can protect in best way , the systems allowing them in the way of causing non damage and eventually fixing the founded vulnerabilities.
d. Ethical hackers deploy their knowledge as risk management techniques.

VIII. PRE-RIQUISIT TO ETHICAL HACKING:

For the purpose to discover the vulnerabilities existing in information systems' operating environments and operating surroundings , Ethical hacking is the methodology adopted by ethical hackers.

One of the better method to evaluate the intruder threat , is to implement professionals attempt in an independent computer security to break their computer systems. Powerful and knowledgeable ethical hackers possess different kinds of skills. They must have to be completely trustworthy mindset in engaging ethical hacking purpose. [4]Ethical hackers typically have very strong programming and computer networking skills.[2] Also adept at installing and maintaining systems which are more popular operating systems (e.g., Linux or Windows 2000) used on targeted systems. Those base skills are augmented with in brief knowledge of the software and hardware provided by the vendors who are popular computer and networking hardware systems.

An ethical hacker's evaluation of a system's security seeks answers to these basic questions[6]:

- Intruder's identifications on the target systems
- Intruder performance for gathered information
- Notice the intruder's at tempts or successes by ending party
- Protective document
- Against actions
- Time, effort, and money willing to expend in obtaining adequate security.

If hired by any organization, an ethical hacker asks the organization what it is trying to protect, against whom, and what resources it is willing to expend in order to gain protection[6]

IX. CONDUCTING ETHICAL HACKING:

The steps followed to conduct Ethical Hacking are as follows:

- Talking to the client about needs of tests.
- Preparation of the documents and asking the client to signature.
- Preparation of an ethical hacking team with drawing up schedule in testing programme.

- Conduct the test in scheduled manner.
- Analyzation of the results and prepare the report accordingly.
- Report delivery to the client.

The 3 components that security evaluation engaged with:

- **Preparation:**In this phase, a formal contract is signed that contains a nondisclosure clause as well as a legal clause to protect the ethical hacker against any prosecution that might be otherwise attract during the conduct phase. The contract also outlines infrastructure perimeter, evaluation activities, time schedules, and resources available to him.[7]
- **Conduct:**In this phase, the evaluation technical report is prepared based on testing potential vulnerabilities. [7]
- **Conclusion:**In this phase, the results of the evaluation are communicated to the organization or sponsors and corrective action is taken if needed.[7]

X.VULNERABILITY RESEARCH

Discovering vulnerabilities and designing weaknesses that will open an operating system and its applications to attack or misuse. It includes both dynamic study of products and technologies and ongoing assessment of the hacking underground. Relevant innovations are released in the form of alerts and are delivered within product improvements for security systems. They can be classified on:

- Security level (low, medium or high)
- Exploit range (local or remote)

Ethical Hackers need vulnerability research for the followings:

- To identify and correct network vulnerabilities
- To protect the network from being attacked intruders
- To get information that helps to prevent problems .
- To gather information about viruses
- To find weaknesses in the network and to alert the network administrators before a network attack
- To know how to recover from a network attack

XI. APPROCHES TO ETHICAL HACKING

Ethical hackers use various methods for breaking the security system in the organizations in the period of cyberattack from other side. Various types of ethical hacks are:

1.Remote Network: This process in especially utilized to recognize the attacks that are causing among the internet. Usually the ethical hacker always tries to identify the default and proxy information into the networks some of them are firewalls, proxy etc.

2.Remote Dial Up Network: Remote dial up network hack identify and try to protest from the attack that is causing among the client modern pool. For finding the open system the organizations will make use of the method called war dialling for the representative dialling. Open system is one of the examples for this type of attacks.

3.Local Network: local network hack is the process which is used to access the illegal information from authorized network by making use of someone with physical access gaining through the local network. To start on this procedure the ethical hacker should ready to access the local network directly.

4.Stolen Equipment: By making use of the stolen equipment hack it is easy to identify the information of the thefts such as the laptops, hard disk etc. the information secured by the owner of the laptop can be identified (Kimberly graves, 2007). Information like username, password and the security settings that are in the equipment are encoded by stealing the laptop.

5.Social Engineering: A social engineering attack is the process which is used to check the reliability of the organization; this can be done by making use of the telecommunication or face to face communication by collecting the data which can be used in the attacks (Bryan Foss and Merlin Stone, 2002). This method is especially utilized to know the security information that is used in the organizations.

6.Physical Entry: This Physical entry organization is used in the organizations to control the attacks that are obtained through the physical premises (Ronald l. Krutz and russel dean Vines, 2007). By using the physical entire the ethical hacker can increase and can produce virus and other Trojans directly onto the network.

7.Application Network: The logic flaws present in the applications may result to the illegal access of the network and even in the application and the information that is provided in the applications.

8.Network Testing: In this process it mainly observes the unsafe data that is present in the internal and the external network, not only in the particular network also in the devices and including the virtual private network technologies

9.Wireless Network Testing: In this process the wireless network reduces the network liability to the attacker by using the radio access to the given wireless network space.

10.Code Review: This process will observe the source code which is in the part of the verification system and will recognize the strengths and the weakness of the modules that are in the software.

11.War Dialling: It simply identifies the default information that is observed in the modem which is very dangerous to the corporate organizations.

XII. DISCUSSION

According to the constructed information for the justification of security in ethical hacking, it is divided into two types as Exposing security transversions must not be rewarded or encouraged and Every company is not consisting of resources to shield existing versions on the system software. Though it might be not certain as the past, the present network systems are significantly dependent on each-other for the aspect of security. One unsecured device placed within a major network can apply as a platform which is up to activate the attacks. The spreded denial of service attack actions are of February 2000 used compromision based hardware devices to flood the Electronic commerce sites in indirect manner. Anyway, each of the computer security is depending on the security of other computers which are situated within the its own community interest. Likewise, the deploying the flaw of security is a positive procedure in both self-interested and public betterment. In consideration with the present site's protection types, the week security on internet, the concept of ethical hacking is the most effective methodology to proactively plug all the identified security chambers and prevent from all the intrusions. Ethical hacking tools like scanners are having notorious type of tools for the crackers. A fine-line having in between hacking to public interest and public community betterment versus leaving tools that might really enable for the attacks and in the aggregates making the internet as unsecure whenever it used to consider in all.

XI I I . DISCUSSION

Network testing is the most important type of ethical hack for keeping information assets secure. The top three benefits of ethical hacks, in order of importance, are improving overall security posture, protecting against theft of intellectual property and fulfilling regulatory/legislative mandates. A majority of IT organizations conduct ethical hacks on wireline and wireless networks, applications and operating systems either annually or more frequently. There is no single set of methodology that can be adopted for ethical hacking. The terms of reference used for various phases in the anatomy of a hack may differ, but the essence is the same. Hacking is not for everyone (there is not half-way). It takes an objective mind, a lot of free time, and dedication to keep up with things. Never use the knowledge for offensive purposes. Lack of experienced staff is most often cited as a significant barrier to conducting ethical hacks internally or improving ethical hacking capabilities. Cost is by far the most common barrier to using an ethical hacking vendor, though most respondents have used this service in the past.

XIV . ACKNOWLEDGMENT

I would like to express my deep gratitude to Dr. Firdous, my research supervisor for his patience guidance, valuable and constructive suggestions during the planning and development of this research paper. His willingness to give his time so generously has been very much appreciated.

I would also like to thank the linkdlin page Cyber Hub for enabling me to follow and observe their daily recaps.

Finally I would like to thank all my batch mates who helped me to encourage in this research paper and my parents for their grateful help.

REFERENCES

[1] Ajinkya A. Farsole, Amurta G. Kashikar and Apurva Zunzunwala , "Ethical Hacking " , International journal of Computer Applications (0975-8887), 2010.

[2] Aman Gupta, Abhineet Anand Student, School of Computer Science and Engineering,Galgotias University,Greater Noida, India amang9578@gmail.com Professor, Department of Computer Science and Engineering, Galgotias University,Greater Noida, India Abhineet.mnnit@gmail.com IJECS Volume 6 Issue 4 April, 2017 Page No. 21042-21050J. International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 6 Issue 4 April 2017, Page No. 21042-21050 Index Copernicus value (2015): 58.10 DOI: 10.18535/ijecs/v6i4.42

[3] Engineering, Guru Nanak Dev Engineering College, Ludhiana, India Ethical hacking: a technique to enhance information security. International Journal of Innovative Research in Science, Engineering and Technology (An ISO 3297: 2007 Certified Organization) Vol. 2, Issue12,December2013.

[4] Halil Ebrahim, Ihsan, Batmaz, "Wireless Network security comparison of WEP mechanism, WPA and RSN security protocols".

[5] 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

[6] James Corley, Kent Backman, and Michael "Hands-On Ethical Hacking and Network Defence", 2006.

[7] Neeraj Rathore, Assistant Professor, Department of Computer Science and Engineering, Jaypee University of Engineering and Technology, Guna, Madhya Pradesh, India. Ethical hacking & security against cyber crime.Article January 2016 DOI: 10.26634/JIT.5.1.4796 .

[8] P. Harika Reddy1 Surapaneni Gopi Siva Sai Teja2 1 Student, Sreenidhi Institute Of Science and Technology, Hyderabad, India. Cyber Security and Ethical Hacking. International Journal for Research in Applied Science & Engineering Technology (IJRASET) ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887 Volume 6 Issue VI, June 2018- Available at www.ijraset.com .

[9] R Rafay Baloch,"Ethical Hacking and Penetration Testing Guide", 2014.

[10] R.R.Schell,P.J.Downey,andG.J.Popek,PreliminaryNotes ontheDesignofSecureMilitaryComputerSystems,MCI-73-1, ESD/AFSC, Hanscom Air Force Base, Bedford, MA (January 1973).