IJCSE International Journal of Computer Sciences and Engineering Open Access

Survey Paper Vol.-7, Special Issue, 4, Feb 2019 E-ISSN: 2347-2693

A Survey on Ethical Hacking Techniques

J. Sathya[1*] , T. Manivannan[2]

[1]Dept. of Computer Science, E.G.S. Pillay Arts and Science College, Nagapatttinam, Tamilnadu, India
[2]Dept. of Computer Science, E.G.S. Pillay Arts and Science College, Nagappatinam,Tamilnadu, India

Corresponding Author: sathyajayakumar33@gmail.com

Available online at: www.ijcseonline.org

***Abstract*—**Hacking is a task in which, a person utilize the weakness in a system for self-profit or indulgence. Ethical hacking is an indistinguishable activity which aims to find and rectify the weakness in a system. In the growing era of internet computer security is of utmost concern for the organizations and government. These companies are using Internet in their wide variety of applications such as marketing, electronic commerce, and database access. But at the same time, data and network security is a serious issue that has to be talked about. This paper attempts to discuss the overview of hacking and how ethical hacking disturbs the security. Also the Ethical Hackers and Malicious Hackers are different from each other and playing their important roles in security. This paper studied the different types of hacking with its phases. The hacking can also be categorized majorly in three categories such as white hat, black hat and grey hat hacking. This paper also presents a comparison of the hacking categories with different methods of penetration testing.

***Keywords*—**Hackers, Ethical Hacking, Hacking Phases.

I. INTRODUCTION

Ethical hacking does perfectly fit into the security life cycle (see figure 1). Ethical hacking is a way of doing a security assessment – a current situation (from a technical point of view) can be checked. Like all other assessments (or audits),an ethical hack is a random sample and passing an ethical hack doesn't mean there are no security issues. An ethical hack's outcome is a complete 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 attackasystemor get access to certain information. With the growth of internet, computer security is of utmost concern for the companies and government. These companies are using Internet in their wide variety of applications such as marketing, electronic commerce and database access. But at the same time, data and network security is a serious issue that has to be talked about. The informationsuch as credit cardnumbers ,telephone numbers, home addresses, bank account numbers etc. that are available on network may easily be hacked by unsocial elements. This is because of the increasing popularity and use of computers, access to them was slender to authorized or agitated personnel. But when some users were refused to access the computer, they would take it oneself, and would summons the access controls. They would steal Password and other information by intruding into the system so as to take control of the whole system. They would do such things just to make happy their ego of not been given the control to access the system, or just for fun, or for money.

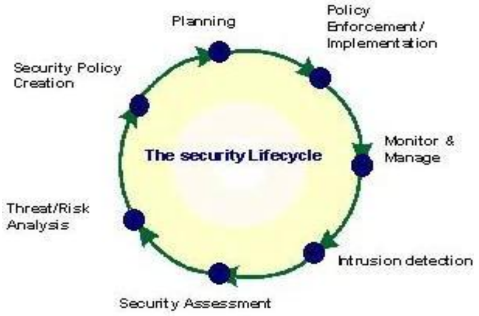


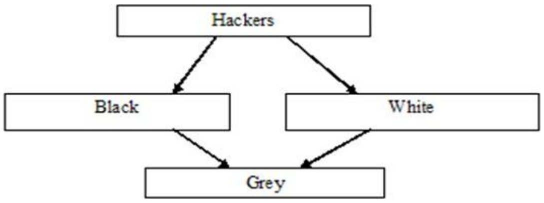
Figure 1: Security Life Cycle

Primarily, these computer intrusions were benign but now they have become a serious matter of security. Sometimes the less capable, or less careful, intruders would unintentionally bring down a system by damaging its files. The system administrator would then have to resume and make repairs to the system. On the other hand, when these intruders were decline access, they would intentionally take devastating actions to harm the organization. When these calamitous computer intrusions increased in number, they became noticeable, picked up by the media and became“news”. The media instead of calling these intruders as “computer criminal,” began to call them as “hackers” and described them as individuals who intrudes into some others' computers, may be for fun orvengeance, or money. At first, “hacker” was meant as an admiration, as this person was well verse with computer programming and knowledge, therefore computer security professionals gave a new term “cracker” or “intruder” for those hackers who used their skills for dark side ofhacking.

To start with hacking, initially organizations decided that the best way to recognize any intrusion into their network or system is to have their own trained professionals who would attempt to break into their systems and would identify, if there are any intrusion threats. These professionals, termed as “Red teams” or “ethical hackers”, follow same steps and tools as that of spiteful hackers, but the difference is of their intensions. Ethical hackers have clear plans to break computer security to save the organization from intrusion attacks. They never reveal the facts and information about the organization. But at any moment of time, if there intensions get sidetracked; they would be the one who would misuse the most. This method of identifying any incursion into the network and systems was also used by United States Air Force. They conducted a “security evaluation” of the Multi-case operating systems for a two-level (secret/topsecret) system. Their assessment found that while Multi-case was notably better than other conventional systems, it also had loop holes in hardware, software and adjectival security. The hackers performed various penetration tests such as information-gathering, to identify any threat that might damage its integrity.

II. TYPES OFHACKING/HACKERS

The hacking can be classified in three different categories. White Hat Hackers are authorized and paid person by the organizations, with good plans and moral standing. They are also known as “IT Technicians” whose job is to safeguard Internet, computer networks, businesses and systems from crackers. Some organizations pay IT professionals to attempt to hack their own servers and computers to test their security. They do hacking for the benefit of the company. They break security to test their own security system. The white Hat Hacker is also called as an Ethical Hacker. In contrast to White Hat Hackers, the aim of Black Hat Hackers is to harm the computer systems and network. They crack the security and adverse effect into the network to harm and destroy data in order to make the network unusable. They deface the websites, plagiarize the data, and crack the security. They crack the programs and passwords to gain entry in the unauthorized network or system. They do those things for their own personal attentiveness like money. They are also known as “Crackers” or Malicious Hackers.



Other than white hats and black hats, an additional form of hacking is a Grey Hat. As like in inheritance, some or all properties of the base class/classes are inherited by the derived class, similarly a grey hat hacker inherits the properties of both Black Hat and White Hat. They are the ones who have morality. A Grey Hat Hacker collects the information and enters into a computer system to breech the security, for the purpose of informing the administrator that there are loop holes in the security and the system can be hacked. Then they themselves may offer the solution. They are well knowledgeable of what is right and what is wrong but sometimes act in a negative direction. A Gray Hat may crack the organizations’ computer security, and may utilize and spoil it. But normally they make changes in the existing programs that can be mended. After sometime, it is themselves who notify the administrator about the company’s security loopholes. They hack or gain unauthorized entry in the network just for fun and not with an intension to harm the Organizations’ network. While hacking a system, irrespective of ethical hacking (white hat hacking) or malicious hacking (black hat hacking), the hacker has to follow some stair to enter into a computer system, which can be talk about asfollows.

HACKING PHASES

Hacking can be done by following Five Phases.

Phase 1:Reconnaissance: In PassiveReconnaissance the Information is gathered regarding the target without Knowledge of targeted company (Or Individual). It could be done simply by penetrating 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, 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 procedure is also called as “Rattling The Doorknobs”. In this method, there is a high risk of being caught as compared to passive Reconnaissance.

Phase 2: Scanning:In this Scanning Phase, The Information collected In Phase 1 Is Used to Examine the Network. Tools likediallers, 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.

Phase 3: Owning 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".

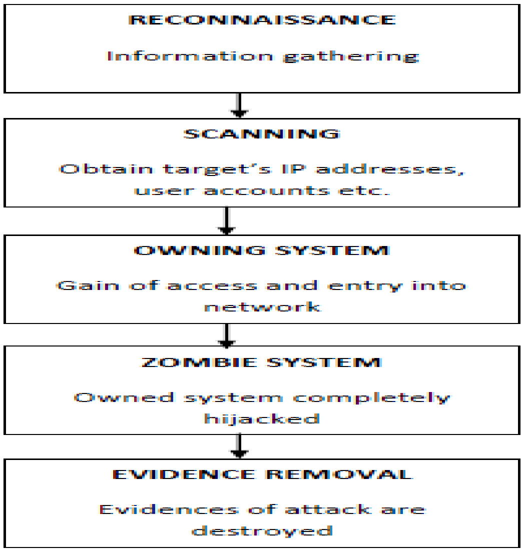

RECONNAISSANCE
Information gathering
SCANNING
Obtain target's IP addresses, user accounts etc.
OWNING SYSTEM
Gain of access and entry into network
ZOMBIE SYSTEM
Owned system completely hijacked
EVIDENCE REMOVAL
Evidences of attack are destroyed

Figure 2: Hacking Phases

Phase 4: 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 "ZombieSystem".

Phase 5: Evidence Removal: Inthis phase, the hacker detach and destroys all the proofs and clues of hacking, such as log files or intrusion detection system alarms, so that he could not be caught and detected. This also protects him from entering into any trial or legality. Now, once the system is hacked byhacker,there is several testing methods are available called penetration testing to discover the hackers and crackers.

III. PHASES OF A PENETRATIONTEST

The overall process of penetration testing can be broken down into a series of steps or phases. The use of an organized approach is important because it not only keeps the penetration tester focused and moving forward but also allows the results or output from each step to be used in the following steps. The use of a methodology allows you to break down a complex process into a series of smaller more manageable tasks. Understanding and following a methodology is an important step in mastering the basics of hacking. This methodology usually contains between four and seven steps or phases. Although the overall names or number of steps can vary between methodologies, the important thing is that the process provides a complete overview of the penetration testing process.

Zero Entry Hacking*: A Four-StepModel*

The first step in any penetration test is reconnaissance. This phase deals with information gathering about the target.

Regardless of the information had to begin with, after completing in depth reconnaissance should have a list of target IP addresses that can be scanned. The second stair in our methodology can be broken out into two distinct activities. The first activity we conduct is port scanning. Once we have finished with port scanning, we will have a list of unsecured ports and potential service running on each of the targets. The second task in the scanning phase is vulnerability scanning. Vulnerability scanning is the process of locating and identifying specific weaknesses in the software and services of our targets. With the consequences from step 2 in hand, we continue to the "exploitation"phase.

Once we know precisely what ports are unsecured, what services are running on those ports, and what vulnerabilities are correlated with those services, we can begin to thrash our target. This is the phase that most newcomers correlate with "real" hacking. Exploitation can involve lots of dissimilar techniques, tools, and code.

In The final phase we will inspect "maintaining access." Often times, the payloads delivered in the exploitation phase provide us with only temporary access to the system. Because most payloads are not uninterrupted, we need to create a more indefinite backdoor to the system. This process permits our administrative access to survive program closures and even reboots. As an ethical hacker, we must be very careful about the use and implementation of this phase. Although not included as a formal step in the penetration testing methodology, the final (and arguably the most important) activity of every PT is the report. Anyway the amount of time and planning you put into conducting the perforation test, the client will often judge your work and effectiveness on the basis of the quality of the report. The final PT report should include all the relevant information uncovered in test and explain in detail how the test was conducted and what was done during the test. Whenever possible, mitigations and solutions should be presented for the security issues you uncovered.

Finally, an executive summary should be included in every PT report. The purpose of this synopsis is to provide a simple one- to two-page, non technical overview of your findings. This report should highlight and briefly summarize the most critical issues your test uncovered. It is vital that this report be readable (and comprehendible) by *both* technical and nontechnical personnel. It is important not to fill the executive summary with too many technical details; that is the purpose of the detailedreport.

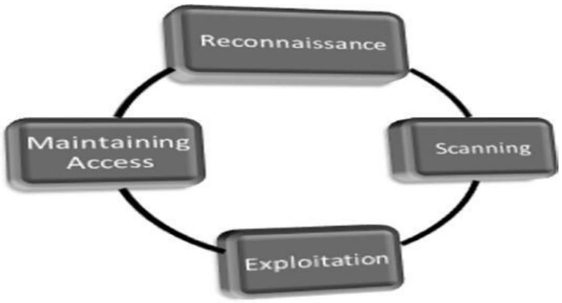


Figure 3: Cyclical Representation of the ZEH Methodology.

IV. WRAPPING UP THE PENETRATION TEST

In many respects, writing the penetrationtestingreport is one of the most critical tasks that an ethical hacker performs. It is important to remember that in many cases, the better you do your job as a penetration tester, the less your client will actually notice or “feel” your work. As a result, the final report is often the only tangible evidence that a client will receive from the penetration tester and the PT process. The penetration testing report often becomes the face of your organization and reputation. Once the initial contract has been signed providing scope and authorization, the penetration tester often disappears from the target organization.

The test itself occurs in a relatively isolated environment. Once the test is completed, it is critical that the penetration tester present his or her findings in a well thought-out, arranged, and easy-to-understand manner. Again, it is important to remember that in most cases the target organization (the company that is paying you) has no concept of what you have been doing or how many hours you have put into the task. As a result, the penetration testing report becomes the principal reflection of your competence. You have a responsibility to the client to present your findings, but you also have an opportunity to showcase your talent and explain how you spent the client’s time and money wisely.

Writing the penetration testing report many penetration testers mistakenly think that they can simply provide the raw output from the tools that they run. This group of people will often collect and neatly organize the various outputs into a single report. They will gather any pertinent information from the reconnaissance phase and include it along with the output from N-map and Nessus. Nessus has severalprebuilt reports that can be generated based off of the scan. Unfortunately, using the prebuilt reports is not enough. Each report must be well laid out and flow as a single document. Combining one style of report from Nessus with a different style of report from NmaporMeta sploitwillmake the penetration test report appear disjointed and unorganized. The penetration testing report needs to be broken into several separate chunks. Taken together, these chunks will form your overall report, but each piece should work as a stand-alone report aswell.

At a minimum, a well-rounded and presented penetration testing report should include the following:

1. An executivesummary
2. A detailedreport
3. R awoutput

Executive Summary

The executive summary should be a very brief overview of your major findings. This document, or sub report, should not exceed two pages in length and only include the highlights of the penetration test. The executive summary does not provide technical details or terminology. This report needs to be written in the context of board members and nontechnical management so that they can understand your findings and any major concerns you discovered on the network andsystems.

If vulnerability and exploits were discovered, the executive summary needs to focus on explaining how these findings impact the business. The executive summary should provide links and references to the detailed report so that interested parties can review the technical nature of the findings. It is important to remember that the executive summary must be very brief and written at a high level. Most executive summaries should be written in such a way that that the report writer’s own grandmother would be able to understand what occurred during the penetration test and what the major findingswere.

Detailed Report

The second part in a well-rounded penetration testing report is the detailed report. This report will include a comprehensive list of your findings as wellas the technical details. The audience for this report includes IT managers, security experts, network administrators, and others who possess the skills and knowledge required to read and comprehend its technical nature. In most cases, this report will be used by the technical staff to understand the details of what your test uncovered and how to address or fix these issues. As with every facet of the penetration test, it is important to be honest and direct with the client. Although it may be tempting to emphasize your great technical savvy and discuss how you owned a particular service, it is much more important to present the facts to your client beginning with the issues that pose the most danger to their networks and systems. Ranking the discovered vulnerabilities can be confusing and daunting for a new penetration tester, luckily most tools like Nessus will provide you with a default ranking system. Always present critical findings first. This makes your penetration test easier to read and allows the client to read about andtakeactionon the most serious findings first (without having to dig through 50 pages of technicaloutput).

Because it is important it needs to be stated again, it is imperative that you put the needs of the client before your ego. Consider the following example: assume you are conducting a penetration test and are able to fully compromise a server on your target's network. However, after further investigation and review, you determine that the newly compromised system is of no value. That is, it holds no data, is not connected to any other systems, and cannot be used to gain further access to the network. Later in the penetration test, one of your tools reports a critical vulnerability on a boarder router. Unfortunately, even after having read the details of the vulnerability and running several tools, you are unable to exploit the weakness and gain access to the system. Even though you are unable to gain access to the boarder router, you are certain that the system is vulnerable. You also know that because this device is a boarder router, if it is compromised the entire network will be atrisk.

Raw Output

The final portion of the report should be the technical details and raw output from each of the tools. In reality, not every penetration tester will agree that this information needs to be included with the penetration testing report. There is some merit to the arguments against including this detailed information, which includes the fact that this information is often hundreds of pages in length and can be very difficult to read and review. Another common argument often repeated from fellow penetration testers is that providing this level of detail is unnecessary and allows the client to see exactly what tools were run to perform the penetration test.

V. BENEFITS OF INDEPENDENTETHICAL HACKING ASSESSMENTS:

1. Complex Enterprise Networks Require Security Expertise

A major challenge for businesses is the complexity of security requirements due to changing hacking strategies, multitude security vulnerabilities, developing business applications, new business technologies, and come forth security technologies. This can guide to large, complex networks that can be difficult to inventory and map. As a result, IT staff can simply overlook or forget about obsolete systems leading to high-risk network entry points. A third-party evaluation will be mandatory to find these overlooked vulnerabilities.

This complexity also creates numerous organization-specific security challenges that are best solved by professionals' with extensive expertise. This expertise is expensive to plough, and ethical hacking companies must put money heavily to develop the skills of their auditors. This enables auditors to maintain an up-to-date repertoire of hacking techniques which ensures accurate assessments and useful recommendations. Businesses can then leverage these expert recommendations to fix security vulnerabilities and implement security tools more effectively.

2. Ethical Hacking Services Provide Objective Analysis andValidation

Ethical hacking offers an objective analysis of an organization's information security posture for organization'sofany level of security expertise. The objectiveness of a security assessment has a direct impact on the value of the assessment. An organization cannot conduct a fair assessment of its security posture due to its preexisting knowledge of security vulnerabilities, security architecture, and the value of target systems. This previous knowledge impacts testing methodology or scope and provides inaccurate evaluation results. By resemblance, hackers have no knowledge of these systems other than what they can collect. Hackers must scan for vulnerabilities, test entry points, eminence targets, and develop a procedure that best influences their resources. An ethical hacking organization is best positioned to amuse this objective and honest evaluation and also offers a fresh perspective to find problems that the customer may be overlooking or omitting. Ethical hacking organizations provide a precious third-party validation of customers' security applications. This is compulsory to demonstrate agreement with industry rules. For example, the payment card industry data security standard (PCIDSS) specification specifies the need for perforation testing once peryear

3.Security as a BusinessEnabler

Security breaches can be very costly yet are difficult to quantify or to forecast. As a result, security is less emphasis for many businesses that would rather invest in revenue-generating technologies. This challenge is further compounded by the pressure for IT organizations to deliver valuable solutions while managing shrinking budgets.

There are many emerging technologies that can provide businesses with operational advantages such as virtualization, cloud computing, and mobile devices. These technologies enable business agility and efficiency but also introduce new security concerns. Due to these new security concerns, businesses should invest in ethical hacking assessments when investing in updated infrastructure or new technologies. These evaluations are essential processes to prevent expensive data breaches that can cost companies in the millions of dollars due to lost business, legal actions or fines. Prescient ethical hacking can prevent these losses and is much more affordable bycomparison.

VI. CONCLUSION

Hacking has both its benefits and risks. Hackers are very different. They may insolvent a company or may secure the data, increasing the profits 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 requires, the malicious hackers violates illegally and harm the network for their personal interest. An Ethical and creative hacking is important in network security, in order to ensure that the company's information is well protected and secure. At the same time it allows the companyto Recognize, and in turn, to take vulnerary measures to remedy the loopholes that exists in the security system, which may permit a malicious hacker to crack their security system. They help companies to apprehend the present hidden problems in their servers and collaborative network. The study also reveals that the authorized users are the ethical hackers, till their aims are clear or else they are a great threat, as they have the access to every piece of information of the organization, as compare to total and semioutsiders.

This also concludes that hacking is an important aspect of computer world. It deals with both sides of being benefits and risks. Ethical hacking plays a vital role in keeping and saving a lot of secret information, whereas malicious hacking can smash everything. What all depends is the intension of the hacker. It is almost unfeasible to fill a slot between ethical and malicious hacking as human mind cannot be conquered, but security measures can be tighten.

REFERENCES

[1] Agarwal, AnkitKumar, Hacking : Research paper, online http://ankitkumaragarwal.com /hacking-a-research- paper/ (visited on may2012)

[2] Wilhelm, Douglas. "2". Professional Penetration Testing.Syngress Press. p. 503.ISBN 978-1-59749-425-0

[3] Moore, Robert (2006). Cybercrime: Investigating High-Technology Computer Crime (1st ed.). Cincinnati, Ohio:

[4] Anderson Publishing. ISBN 978-1-59345-303-9

[5] EC-Council (n.d.). Ethical Hacking and Countermeasures, online http://www.eccouncil.org/ipdf/EthicalHacker.pdf (visited on may 2012)

[6] Ethical Hacking Basics Class part , online http://www.go4expert.com/forums/ showthread.php?t=11925 (visited on may 2012)

[7] Palmer, C.C.(2001,April 13). Ethical Hacking. IBM Systems Journal Vol. 40 No.3 2001

[8] Http://1000projects.org/how-is-ethical-hacking-done-cs- student-project-seminar.html

[9] en.wikipedia.org/wiki/Penetration_testing

[10] About Effective Penetration Testing Methodology byByeong-Ho KANG