WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Study of Ethical Hacking

Abijithv.M[1], Sanjay Mohan[2]

[1]UG Student Computer Science Department,Sri Krishna Arts And Science College,CBE.
[2]UG Student Computer Science Department,Sri Krishna Arts And Science College, CBE
[1]E-MAIL: abijithvm21bds002@skasc.ac.in
[2]E-MAIL:sanjaymohan21bds040@skasc.ac.in

ABSTRACT

The online security situation is very bad. Robbery is an activity where, one uses weakness a for-profit or self-satisfaction program. As public and private organizations move beyond their core functions or applications such as e-commerce, marketing and Internet access, and criminals have more the opportunity and motivation to access sensitive information through the Web application. So the need for protection systems ranging from hijackers produced by hijackers to encourage people to retaliate against illegal attacks our computer systems. Direct robbery is the same activity that aims to detect and correct weaknesses once and for all system vulnerabilities. Ethical Hacking describes the process of hacking the network in a moral way, so with good intentions. This paper explains what Ethics Hacking is, what types of behavioral fraud, the impact of hijacking. Businesses & Governments. This paper has learned the different types of scams by your categories.

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

1.INDRODUCTION

Ethical hacking :it is defined as the practice of robbery without any intention of harm. The Ethical Hackers and Malicious Hackers are differentwith each other and play their important rolesecurity.According to Palmer (2004, as quoted by Pashel,2006): "Moral hijackers use the same tools againtactics as attackers, but they do not hurttargeted systems or information theft. Instead, they exploresecurity of targeted systems and report to owners viaweaknesses they found and instructions on how to do itfix it". The great growth of theinternet has broughtmany good things like electronic trading, email, easyaccess to major reference stores etc. Like, and manytechnological advances, there is another side: crimehackers who will secretly steal the organizationinformation and transfer it to the open internet. These typesof hijackers are called black hat hackers. So, victory fromthese serious problems, another class of hijackers enteredexistence and these hackers are called ethical hackers orwhite hat hackers.

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 securit 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 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. We can easily say that Ethical hacking does perfectly fit into the security life cycle.

Fig. 1 – Ethical Hacking

TYPES OF HACKING/HACKERS

The hacking can be labeled in three extraordinary classes, in step with the shades or colorations of the Hat". The phrase Hathasits beginning from vintage western films wherein the color of Hero's' cap changed into "White" and the villains'cap turned into "Black". It may also be said that the lighter the color, the much less is the intension to harm.

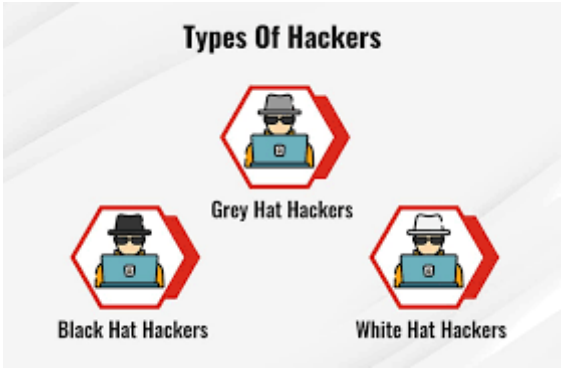

Fig. 2 – Types of Hackers

1.1 White Hat Hackers

White Hat Hackers are company-authorized and paid individuals with noble intentions and moral standing. "IT Technicians" is another name for them. Their goal is to keep crackers out of the Internet, businesses, computer networks, and systems. To evaluate its security, several firms hire IT professionals to attempt to hack their own servers and PCs. They do hacking for the company's profit. They test their own security mechanism by breaking it. Ethical hackers are also known as white hat hackers. White Hat Hackers are the opposite.

1.2 Black Hat Hackers

Black Hat Hackers aim to do harm to computer systems and networks. They breach security and infiltrate the network in order to hurt and destroy data and render the network unusable. They deface websites, steal information, and compromise security. To obtain access to the unlawful network or system, they crack the programmes and passwords. They do activities for personal gain, such as making money. "Crackers" or "Malicious Hackers" are other names for them. Aside from white and black hats.

1.3 Grey Hat Hackers

Grey Hat hacking is another type of hacking. As with inheritance, the derived class inherits part or all of the properties of the original class/classes; similarly, a grey hat hacker inherits the properties of both Black Hat and White Hat. They are the ones with morals. A Grey Hat Hacker obtains information and breaks into a computer system to breach security in order to alert the administrator about security flaws and the system's vulnerability to hacking. They may then offer the cure themselves. They are fully aware of what is good and wrong, but they occasionally act in a negative manner. A Gray Hat could compromise an organization's computer security, exploiting and defacing it. However, they frequently create alterations to existing programmes that may be fixed. After a while, They are the ones who notify the administration.a company's security flaws They gain or hack illegal network access for entertainment purposes only a desire to cause harm to an organization's network While Regardless matter whether the hacking is ethical (white hat),Hacking (white hat hacking) or malicious hacking (black hat hacking),To gain access to a computer, a hacker must take certain actions.As anexample, consider the following system.

2. HACKING PHASE

Fig. 3 – Hacking Phase

Hacking Can Be Done According to The Five Steps:

Step 1: Reconnaissance: may be activated or logged into re-evaluate the information collected about the target without the knowledge of the target company (or individual). It can be done easily search for information of the target online or bribe an employee of the target company who will also disclose provide useful information to the gang. This process is also called "information gathering". In this method, hacker does not attack the system or network ofcompany to collect information. Although it worksnote, hacker logs into the network to find outindividual hosts, ip addresses and network

services. Thisprocess is also called “door-to-door lizards”. In thisway, there is a higher risk of being caught comparedpassive processing.
Step 2: Scanning: In the scanning section, Information Compiled in Section 1 Used for Network Exploration. Tools Like Dialers', Port Scanners Etc. used by Network Explorer Hacker To Get Access System and Company Network.
Step 3:Gaining Access: This Is Real and Real hacking category. Hacker uses Acquired Information Previously Two Phases In Attack And Invasion Local Network (LAN, Wireless or Wireless), Local Pc Access, online or offline. This Section Is Also Called “Program Management”
Step 4: Maintaining Access: Once the hacker has won access to a system or network, you retain that access future attacks (or additional attacks), by doing changes in the system in such a way that some hackers or security people are unable to enter and reach the victims system. In such a case, the managed system (referred to in Phase 3) is then called the “Zombie System”.
Step 5: Clearing Track: At this stage, hacker removes and destroys all evidence and details of the robbery, such as log files or Access System Alarms, so that he may be arrested and pursued. This saves him at the entry of any trial or formal hearing. Now, once the system hacked by hacker, there are a few ways to test available so-called entry check for hackers and crackers.

3.IMPACT OF HACKING ON BUSINESSESANDGOVERNMENTS

Some of the most expensive and most expensive victims robbery into businesses. Businesses many times targeted to their personal and financial customer data as well usually aimed at their own employees, or dissatisfied or opportunistic. Businesses lose billions dollars a year for hijacking and other computers violations. Most of the time, the actual cost cannot be estimated because the consequences of security breaches can last for years after a real attack. Companies can lose customers self-confidence and in many cases have a legal obligation any loss to their customers. Recovery costs fromattacks can spread quickly: legal fees, investigative fees, stock performance, reputation management, customer support, etc. Companies, and more recently, consumers, are investing extra money to prevent an attack before it actually happened. Businesses that own consumer stores personal and financial data in particular take additional steps to ensure data security. Microsoft Online Team, MSN / Windows Live, requires no more than one group store Personal identification information without explicit consent in the internal security team. Security updates are possible regularly in groups that store consumer data and the security team performs its own personal safety update by doing you are actually trying to access sites. Sites they actually had held from download to web because of errors found in this way. Some businesses are very limited in technical areas they have hired external security experts to assist for their safety. ScanAlert.com prides itself on performance with more than 75,000 secure ecommerce sites, including manypopular brands such as Foot Locker, Restoration Hardware and Sony. Ecommerce sites that hold the logo “Hacker Safe”, meaning that the site is inspected daily and operates effectively 99.9% hacker crime prevention. Disclaimer Scan Alert sentence although it seems to have very little confidence:This information intended as a related indicator of safety efforts for this website and its operators. While this, or the other, risk assessment does not and does not guarantee safety;indicates that [e-Commerce Site] meets all credit card industry risk guidelines for remote web servertesting to help protect your personal information hijackers. HACKER SAFE does not identify hacker evidence. The HACKER SAFE certificate cannot and does not protect any of your data that may be shared with other servers that HACKER SAFE is not guaranteed, such as a credit cardprocessing networks or data storage offline, and does not protects you in some ways your data may be illegal was detected as access to a non-Internet "insider". While Scan Alert makes reasonable efforts to verify its certification service is running smoothly, Scanning notification does not warranty or claim of any kind, whatever, about the accuracy or usefulness of any information provided herein. By using this information you agree that the Scanner Notice will be caught harmless in any incident.

2.1 Benefits of Ethical Hacking

- This type of “testing” can provide compelling evidenceof the actual system or network threatswith proof of access. Although these benefitsit may be negative in some way, by pointing to eitherexposure can be active in developmentcomplete security of your systems.

- However, information security should not be strictly limited to the mechanics of hardening networks and computer systems. A mature security information program is a combination of policies, procedures, technical system and network standards, configuration settings, monitoring, and auditing practices. Business systems, which have resisted simple, direct attacks at the operating system or network level, may succumb to attacks that exploit a series of procedural, policy, or people weak points.

- A hack of good principles, which explores beyond the operating systemand network vulnerability, for example,your hack of conduct should prove that your firewallshe could not resist the attack because it was not thereviolation, but no one realized the attack, you may havebetter prepared to make a development case gaining access to a broader organizational perspectivesecurity. The results should give a clear picture how well your recovery processes work as well responses that should be present. This type of “experiment” may also reveal such weaknesses such as the fact that many security managers of systems may not recognize the tactics of the robbery as it really is to hackers trying to protect themselves from them. These findings can help improve the need to do better communication between program managers and technical support staff, or identify training needs.

- Often, adult safety awarenessmanagement is very limited.communicative diagnostic work is primarily concernedit can be a threat and this often leads to casualtiesthe idea of a threat, to postpone demand immediately

addressing needs. By moral fraudexercise, especially if the results arenegative, highmanagers will have a greater understanding of problems and better able to prioritizerequirements. To improve access.

2.2 Limitations of Ethical Hacking

- Ethical hacking is based on a simple principle of detect security risks to systems once networks before hackers do, through so-called "Hacker" strategies to get this information. Unfortunately, such common definitions testing usually stops operating systems, security settings, and "bug" level. Limiting I test yourself at the technical level by making a series for technical testing only, a proper robbery job no better than the "diagnostic" limit of the system security.

- Time is also an important factor in this type of testing.Hackers have a huge amount of time and patiencewhen you detect system crashes. Probably youit will involve a"trusted foreign company" to play these tests are for you, so your time is money. Other the consideration in this is that in using the "third person" in orderyou will do tests, you will be providing "insideknowledge "to speed up the process and savetime. The chance of being found may be limitedas testers can only work through information provided.

- An additional limitation of this type of test is thatit usually focuses on the outer rather than the inner,therefore, you may only get half ofnumber. If it is not possible to test the systeminternally, how can that system be established"safe from attack", based on external testing?Basically this kind of test alone will never endto provide full security guarantees.Therefore, such testing strategies may be obvious,initially, to be flawed and limitedvalue, because all risks may be non-existentuncovered.

3.CONCLUSION

Hacking has its advantages and disadvantages. The hackers they are very diverse. They may pay the company or they may protect data, increase company revenue. War between criminals of character or white hat once vicious or black hat hackers are a long, useless warthe end. Although good criminals help to understand their corporate security needs, malicious hackers enterillegally and damages the network for its own benefits. which may allow a dangerous criminal to break the law their security system. Ethical Hackers help organizations to understand current hidden problems on their servers and the business network. Ethical hacking is a tool, which Used properly, it can do much good network vulnerabilities and how they can be exploited. [2] This also concludes that robbery is an important element in the computer world. It deals with both the sides of being good and bad. Ethical Hacking plays an important role roles of storing and storing large amounts of confidential information, and vicious robberies can ruin everything. This it all depends on the thickness of the hacker. Probablyit is impossible to bridge the gap between good and bad behaviorrobbery as the human mind cannot be defeated, but security steps can be strengthened.

REFERENCES

[1] Eleventh LACCEI Latin American and Caribbean Conference for Engineering and Technology (LACCEI'2013)

[2] K.BalaChowdappa et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (3) , 2014, 3389-3393

[3] Gurpreet K. Juneja,"Ethicalhanking :A technique to enhance information security"international journal of computer applications(3297: 2007),vol. 2,Issue 12,december2013

[4] Kumar Utkarsh" SYSTEM SECURITY AND ETHICAL HACKING"

[5] Wikipedia

[6] "Innovation in Engineering, Technology and Education for Competitiveness and Prosperity" August 14 - 16, 2013 Cancun, Mexico. "Faculty Attitudes Toward Teaching Ethical Hacking to Computer and Information Systems "Undergraduates Students Aury M. Curbelo, Ph.D,Alfredo Cruz, Ph.D.