ETHICAL HACKING

SEMINAR REPORT

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR
THE
DEGREE
OF
MASTER OF COMPUTER APPLICATIONS

DEPARTMENT OF MATHEMATICAL AND COMPUTATIONAL SCIENCES

NATIONAL INSTITUTE OF TECHNOLOGY

KARNATAKA

SURATHKAL, MANGALORE-575025

JANUARY, 2020

SUBMITTED BY	**SUBMITTED TO**
DIVAS KUMAR	DR. VISHWANATH K.P
194CA019	Mr. ANITA SR
MCA 2nd SEM	

DECLARATION

I hereby declare that the seminar reports entitled **“ETHICAL HACKING”** which is being submitted to the National Institute of Technology Karnataka, Surathkal, in partial fulfillment of the requirements for mandatory learning course (MLC) of **Master of Computer Applications** in the **Department of Mathematical and Computational Sciences,** is a bonafide report of the work prepared by me. The material is collected from various sources with utmost care and is based on facts and truth.

DIVAS KUMAR
194CA019
MCA 2nd SEM
NITK, SURATHKAL

CERTIFICATE

This is to certify that the P.G. Seminar Report entitled **“ETHICAL HACKING”** submitted by **‘DIVAS KUMAR’** (Roll No :- 194CA019) as a record of the work carried by him is accepted as the P.G. Seminar Work Report submission in partial fulfillment of the requirements for mandatory learning course of **Master of Computer Applications** in the **Department of Mathematical and Computational Sciences.**

ABSTRACT

Ethical hacking is the way to find out the weaknesses and vulnerabilities in the system or computer network. It is a way to describe the procedure of hacking in an ethical way for any network. The ethical hacker has a good purpose to do it. Actually it has become the general perception in our mind for hackers that he will be bad, fanatic, criminal and unethical. Basically some of the hackers have even done very badly with some organisations like they have stolen very important information from their customers. In some of the government organisations they have damaged very confidential information like social security numbers and other sensitive information. That is the reason hackers are not having very good reputation. To avoid such conditions many organisations have hired many ethical hackers to keep a track on their system and computer network. Ethical hackers are supposed to test and check vulnerabilities and weaknesses in the present system. There is another face of the coin which tells that without hackers the vulnerabilities and holes of software would remain undiscovered. In this paper I have tried to explain the good and bad face of hackers and even of ethical hackers also and what are the different impacts on the different areas of our society. I have tried to explore the moral behind ethical hacking and the problems lie with this particular field of information technology where security is concerned. There are several fields in computing where hackers made measurable impact on society.

CONTENTS

1. WHAT IS HACKING

Hacking is identifying weaknesses in computer systems or networks to exploit its weaknesses to gain access. Hacking means using computers to commit fraudulent acts such as fraud, privacy invasion, stealing corporate/personal data, etc.Example of Hacking: Using password cracking algorithm to gain access to a system.

Computers have become mandatory to run a successful business. It is not enough to have isolated computer systems; they need to be networked to facilitate communication with external businesses. This exposes them to the outside world and hacking. Cyber crimes cost many organizations millions of dollars every year. Businesses need to protect themselves against such attacks.

1.1 Hackers

A hacker is an individual who uses computer, networking or other skills to overcome a technical problem. The term hacker may refer to anyone with technical skills, but it often refers to a person who uses his or her abilities to gain unauthorized access to systems or networks in order to commit crimes.

1.2 Types of Hackers

- Black Hat Hacker
- White Hat Hacker
- Grey Hat Hacker
- Script kiddies
- Hacktivist
- Phreaker

Black Hat Hacker

Black hat hackers are individuals with extraordinary computing skills, resorting to malicious or destructive activities. That is black hat hackers use their knowledge and skills for their own personal gains probably by hurting others. These black hat hackers are also known as crackers.

White Hat Hacker

White hat hackers are those individuals professing hacker skills and using them for defensive purposes. This means that the white hat hackers use their knowledge and skill for the good of others and for the common good. These white hat hackers are also called security analysts.

Grey Hat Hacker

These are individuals who work both offensively and defensively at various times. We cannot predict their behaviour. Sometimes they use their skills for the common good while in some other times he uses them for their personal gains.

Script kiddies

A non-skilled person who gains access to computer systems using already made tools.

Hacktivist

A hacker who uses hacking to send social, religious, and political, etc. messages. This is usually done by hijacking websites and leaving the message on the hijacked website.

Phreaker

A hacker who identifies and exploits weaknesses in telephones instead of computers.

1.3 Hackers vs Crackers

Hackers are constantly looking for the flaws in the computer and internet security and their sole aim is to rectify these flaws and improve the security of the content.There is a common view that the hackers build things.

Crackers are those who break the security of computers and networks.The crackers are believed to break the things. Crackers break the security system for criminal and illegal or for personal gains.

1.4 Famous hackers

While many famous technologists have been considered hackers, including Edward Snowden, Aaron Swartz, Donald Knuth, Ken Thompson, Vinton Cerf, Steve Jobs and Bill Gates, black hat hackers are more likely to gain notoriety as hackers in mainstream accounts. Gates was also caught breaking into corporate systems as a teenager before founding Microsoft.

2. ETHICAL HACKING

Ethical hacking refers to the act of locating weaknesses and vulnerabilities of computer and information systems by duplicating the intent and actions of malicious hackers. Ethical hacking is also known as penetration testing, intrusion testing, or red teaming. An ethical hacker is a security professional who applies their hacking skills for defensive purposes on behalf of the owners of information systems.

Hacking can be legal if done with permission. Computer experts are often hired by companies to hack into their system to find vulnerabilities and weak endpoints so that they can be fixed. This is done as a precautionary measure against legitimate hackers who have malicious intent. Such people, who hack into a system with permission, without any malicious intent, are known as ethical hackers and the process is known as ethical hacking.

The International Council of E-Commerce Consultants (EC-Council) provides a certification program that tests individual's skills. Those who pass the examination are awarded with certificates. The certificates are supposed to be renewed after some time.

2.1 Why Ethical Hacking?

Information is one of the most valuable assets of an organization. Keeping information secure can protect an organization’s image and save an organization a lot of money.

Hacking can lead to loss for business organizations that deal in finance such as PayPal, Paytm etc.

An Ethical hacker will first think with a mindset of a hacker who tries to get into the system.If he succeeds in penetrating into the system then he will report to the company with a detailed report about the particular vulnerability exploiting which he got into the system.

2.2 Types of ethical hacking

Ethical hackers use various methods for breaking the security system in the organizations in the period of cyber attack. Various types of ethical hacks are:

Remote Network: This process is 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 in the networks some of then are firewalls, proxy etc.

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

Stolen Equipment: By making use of the stolen equipment hack it is easy to identify the information of the thefts such as the laptops 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.

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. This method is especially utilized to know the security information that is used in the organizations.

Physical Entry: This Physical entry organization is used in the organizations to control the attacks that are obtained through the physical premises. By using the physical entire the ethical hacker can increase and can produce virus and other Trojans directly onto the network.

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.

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.

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.

3. TOOLS AND TECHNIQUES

Hacking Tools are computer programs and scripts that help you find and exploit weaknesses in computer systems, web applications, servers and networks. There is a variety of such tools available on the market. Some of them are open source while others are commercial solutions.

Netsparker

Netsparker is an easy to use web application security scanner that can automatically find SQL Injection, XSS and other vulnerabilities in your web applications and web services. It is available as on-premises and SAAS solution.

Acunetix

Acunetix is a fully automated ethical hacking solution that mimics a hacker to keep one step ahead of malicious intruders. The web application security scanner accurately scans HTML5, JavaScript and Single-page applications. It can audit complex, authenticated web apps and issues compliance and management reports on a wide range of web and network vulnerabilities.

Burp Suite

Burp Suite is a useful platform for performing Security Testing of web applications. Its various tools work seamlessly together to support the entire pen testing process. It spans from initial mapping to analysis of an application's attack surface.

Aircrack

Aircrack is a trustworthy ethical hacking tool. It cracks vulnerable wireless connections. It is powered by WEP WPA and WPA 2 encryption Keys.

Angry IP Scanner

Angry IP Scanner is an open-source and cross-platform ethical hacking tool. It scans IP addresses and ports.

Hashcat

Hashcat is a robust password cracking ethical hacking tool. It can help users to recover lost passwords, audit password security, or just find out what data is stored in a hash.

SQLMap

SQLMap automates the process of detecting and exploiting SQL Injection weaknesses. It is open source and cross platform. It supports the following database engines.

3.1 Common Methods used in Ethical Hacking

Some of the most common methods used in Ethical Hacking are :

SQL injection

A SQL injection is an attack in which computer code is inserted into strings that are later passed to a database.

A SQL injection can allow someone to target a database giving them access to the website. This allows the person to extract the content from the database that may be text, audio, video or images.

Adware

Adware refers to any software program in which advertising banners are displayed as a result of the software's operation. This may be in the form of a pop-up or as advertisements displayed on the side of a website, such as on Google or Facebook.

Phishing

Phishing refers to the dishonest attempt to obtain information through electronic means by appearing to be a trustworthy entity.

Ransomware

Ransomware is a type of malicious software that prevents the user from accessing or using their data (often through

encrypting the data), whereby a fee must be paid or service performed before the user's data is decrypted.

Malware

A simplistic definition of malware is malicious software. Malware, for the purpose of this research, is defined as potentially harmful software or a component of software that has been installed without authorization to a third-party device.

Virus

A virus is a "block of code that inserts copies of itself into other programs." Viruses generally require a positive act by the user to activate the virus. Such a positive act would include opening an email or attachment containing the virus

Worm

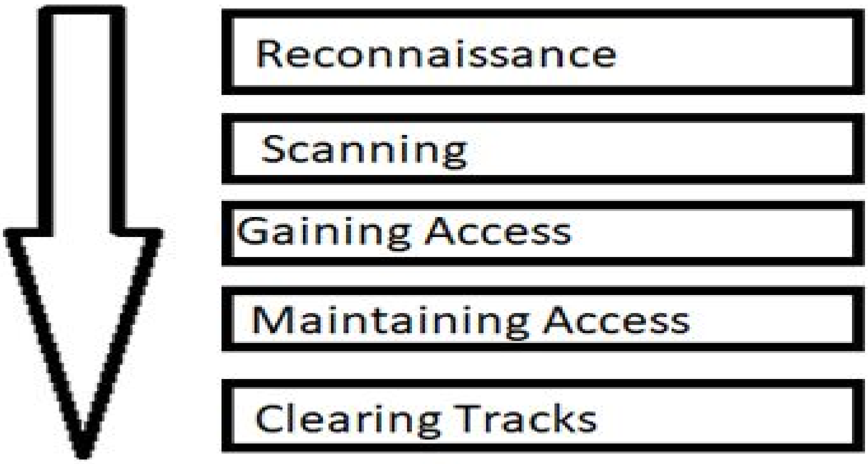
A worm is a program that propagates copies of itself over networks. It does not infect other programs, nor does it require a positive act by the user to activate the worm. It replicates by exploiting vulnerabilities.

Password Cracking

There are many methods for cracking the password and then get in to the system. The simplest method is to guess the password. But this is a tedious work. But in order to make this work easier there are many automated tools for password guessing like legion. Legion actually has an inbuilt dictionary in it and the software will automatically generate the password using the dictionary and will check the responses.

3.2 Phases of Hacking

There are mainly five phases in Hacking. It is not necessarily a hacker has to follow these five steps in a sequential manner. It's a stepwise process and when followed it gives a better result.



1. Reconnaissance

Reconnaissance is the first phase of Hacking. It is also called as Footprinting and information gathering phase. In this phase we collect as much information as possible about the target.

There are two types of Footprinting:

Active: Directly interacting with the target to gather information about the target.

Passive: Trying to collect the information about the target without directly accessing the target. This involves collecting information from social media, public websites etc.

2. **Scanning**

Three types of scanning are involved:

Port scanning: This phase involves scanning the target for the information like open ports, Live systems, various services running on the host.

Vulnerability Scanning: Checking the target for weaknesses or vulnerabilities which can be exploited. Usually done with the help of automated tools.

Network Mapping: Finding the topology of network, routers, firewalls servers if any, and host information and drawing a network diagram with the available information. This map may serve as a valuable piece of information throughout the hacking process.

3. **Gaining Access:**

This phase is where an attacker breaks the system/network using various tools or methods. After entering into a system, he has to increase his privilege to administrator level so he can fetch the information that needed or modify data or hide data.

4. **Maintaining Access:**

Hackers need to maintain or persist the connection in the background without the knowledge of the user. This can be done using Trojans, Rootkits or other malicious files. The aim is to maintain the access to the target until he finishes the tasks he planned to accomplish in that target.

5. **Clearing Track:**

No thief wants to get caught. An intelligent hacker always clears all evidence so that in the later point of time, no one will find any traces leading to him. This involves modifying/corrupting/deleting the values of Logs, modifying registry values and uninstalling all applications he used and deleting all folders he created.

3.3 Skills required

Programming skills

All the websites and all types of software have been developed by different programming languages. Hacking is all about gaining access to the foundation of the software. In order to access this foundation, you need to have a proper understanding of the programming language that was used to develop the software.

Linux

Most web servers are run on the Linux operating system. As an ethical hacker, one of your most frequent roles will be to gain access to the server. This automatically makes Linux a must-have skill for ethical hacking. You should have an in-depth knowledge and understanding of this operating system.

Cryptography

Cryptography is all about transforming a normal text into a non-readable form and vice versa.In terms of security, cryptography promotes integrity, confidentiality, and authenticity. As a hacker, you may also be required to decrypt some suspicious messages.

Database Management System (DBMS)

DBMS is a software and protocol that are used for creating and managing databases. One of the things that most hackers target is the database. This is because all the information that is needed is likely stored in the database. As an ethical hacker, you need to exploit the vulnerabilities and security threats of different databases.

Networking Skills

Most security threats originate from networks. This makes computer networking an essential skill that should be learned by any aspiring ethical hacker. You should have a deep understanding of how computers in a network are interconnected. You should also be good at exploring all the security threats that may be existing in a network and how to handle them.

4. Advantages and Disadvantages

Ethical Hacking nowadays plays a vital role in Network security. Although as everything has some pros and cons, some of the major pros and cons of ethical hacking are as follows.

- Helps in closing open holes in the system network.
- Provides security to banking and financial organisations.
- Prevents website defacements
- Trustworthiness of the Ethical hackers is important.
- Hiring professionals is expensive.

5. Future scope of Ethical Hacking

- Ethical hackers are hired to find any vulnerability that might exist in a network and to fix them.
- IT firms are the main recruiters of ethical hackers. They can also be required by financial service providers, airlines, retail chains and hotels.
- Some skilled hackers work for investigative agencies like the Central Bureau of Investigation, the National Security Agency and the Federal Bureau of Information.
- Some large organisations employ security testers and others use contractors to audit their systems.

6. Conclusion

This report looked at the good and bad things about ethical hacking where we have white hat hackers, they are known as ethical hackers. Then we have black hat hackers, who are the criminal's of the internet. We also have the hacktivists, who break into websites and deface them by changing the content of the website. I also discussed why ethical hacking is important and how they really help and hinder society. I also discussed different types of ethical hacking and tools for breaking the security system of the organizations in the period of cyber attack. There are various common methods used in ethical hacking, some of them are SQL injection, Adware, Phishing, Password cracking etc. There are basically five phases of hacking which need to follow for better results. Ethical hacking has some advantages, where they protect company's data, and some of the disadvantages where ethical hackers have ended up in jail for hacking.

The field of ethical hacking will see exponential growth in the coming years as the world is moving towards a digital economy and the growing industries in every sector are going to need cyber security specialists in the form of ethical hackers to keep their systems safe and out of the reach of black hat hackers.

7. References

1. **Miles Price, Hacking: The Beginner's Complete Guide to Computer Hacking and Penetration, (An introduction to hacking)**
2. **EC-Council University (2019). " Learn the 5 phases of Ethical Hacking", https://www.eccu.edu/learn-the-5-phases-of-ethical-hacking/ (Feb. 13, 2020).**
3. **Krishna Rungta (). "Free Ethical Hacking Tutorials: Course for Beginners", https://www.guru99.com/ethical-hacking-tutorials.html(Feb. 13,2020).**
4. **Jobs. Mohtashim M (). "Ethical Hacking Tutorial", https://www.tutorialspoint.com/ethical_hacking/index.htm(Feb. 13,2020).**
5. **Aryya Paul (May 22,2019). "An Introduction to Ethical Hacking", https://www.edureka.co/blog/what-is-ethical-hacking/#What-is-Ethical-Hacking (Feb. 13,2020).**
6. **Wikipedia (2012). "Security hacker", https://en.wikipedia.org/wiki/Security_hacker(Feb 14, 2020).**