Ethical Hacking and its Necessity in the Society

By

Gulfraz Naqvi
University of Management & Technology, Lahore, Pakistan
Email: gulfraz.naqvi@umt.edu.pk

Hamdan Sultan
University of Management & Technology, Lahore, Pakistan
Email: hamdan.sultan256@gmail.com

Abstract

Hacking mostly known as a way to steal one's privacy and confidential information for some benefit, a breach in the system causes this type of immense damage. But hacking with good intentions and benefits to someone is known as ethical hacking. Ethical hacking is a method to find vulnerabilities in one's system or network. Ethical hackers are individuals who use proper standards to find these vulnerabilities in a legit way. Most people considered hacking as a bad, unethical practice and refer to most as criminals, because most individuals have disrupted organizations and stole confidential information, money and other important files concerning that organization. Due to this reason many organizations and even the government decide to recruit the ethical hackers to discover the vulnerabilities in their system and network. There is one another face of the coin which tells that without hackers the vulnerabilities and holes of software would remain undiscovered. In this research paper I have tried to explain the benefits of this type of hacking, how it has impacted our today's society and what can be considered an ethical and unethical hacker. In this research paper I have attempted to find the problem that currently affect this field where security and vulnerability are most concerned. And how this form is hacking is affecting our modern-day society.

Keywords: Ethical hacking, hackers, hacking, Security.

Introduction

Ethical hacking is a legit way to find vulnerabilities in a system or network. Ethical hackers use their abilities to find and investigate these security problems that other malicious hackers try to exploit. Though this method uses the same tools and techniques as regular hacking, but it is done by the organization or the individual's consent. Because of smartness of hackers, ethical hacking arose as the latest and innovative computer technology **[2].**

It is hard to understand the true intentions of the public, and due to this fact, it is difficult to acknowledge the motives of ethical hackers that are finding these vulnerabilities in our system or network. Since the rise of cybercrime most organization are hiring ethical hackers also known as white hackers. But these ethical hackers also have their opposites known as the "black hackers". These individuals are complete opposite of ethical hackers and are only have malicious intent, their end goal is to make profit by any means.

Ethical Hacking

Ethical hackers

Ethical hacking is an authorized way to expose the vulnerabilities of a system or network and to make them secure for the organization been affected by these potential data breaches. Ethical Hackers are certain individuals who have expert abilities that aim to investigate the weak points in a vulnerable system from malicious hackers. They collect the information they find from these data breaches and find out ways to enhance the security of system or network.

Once these vulnerabilities are eliminated, users are notified and need to explore and improve their security and determine how a hacker breached their networking system. To be safe in this internet world, user needs to learn how a hacker (cracker) can get into his network **[3].**

Methodology of Ethical hacking

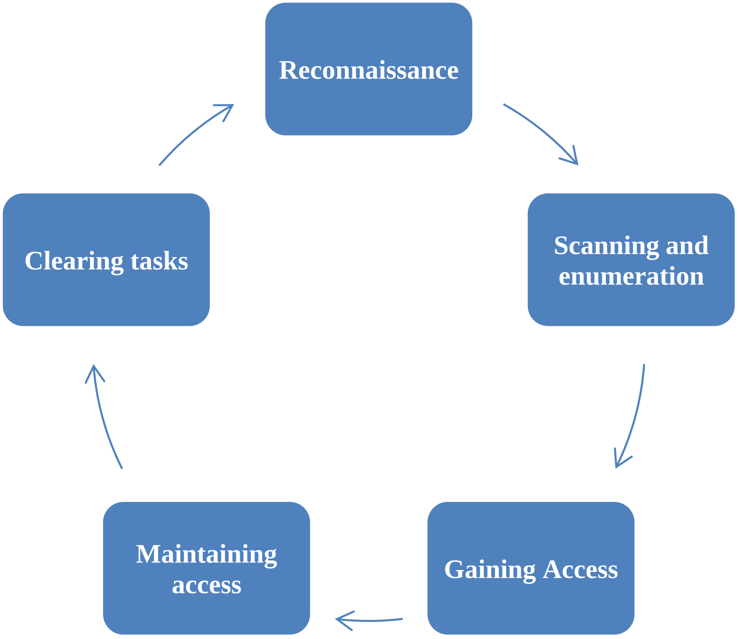

Figure 1: *Ethical hacking methodology*

Reconnaissance

The initial phase in which any hacker gathers information about an individual or an organization secretly, dumpster diving is a phase where the hacker collects old passwords, documents and other important files from the targeted system. The next phase foot printing collect data from security in the system, reducing the need of to find a certain IP address in the vulnerable system. Ethical hacker uses these phases to gather information about the client or organization's system, following the seven steps mentioned beneath **[4].**

- Information Gathering
- Mapping the Network
- Determining the network range Identifying the active machine
- Identification of open ports and access points
- OS fingerprinting
- Fingerprinting Services
- Identification of the active machine

Tools used in Reconnaissance

Who is Lookup and NSlookup.

Scanning and enumeration

During this phase an ethical hacker uses different methods to find back door in a system or network. We scan against a client where the hacker looks for open ports and vulnerabilities. They are required to find out network topologies, routing, firewall, live services.

Tools used for scanning

Namp, Zenmap, Nikto

Gaining Access

Once the hacker gathers all the necessary information related to the system vulnerabilities, they attempt to gain access of the affected network.

Tools for gaining access

John the ripper, Aircrack, Cain and Abel

Maintaining access

After gaining access to the infected system, the hacker can install rootkit at a kernel level of the operating system which will aid them to have full access of the system or network. While they will use trojan to extract user passwords and sensitive information, credit card information.

Tools used for maintaining access

Metasploit Penetration testing software

Clearing tasks

The last phase of the methodology where all the relative data of a system breach by the hackers are deleted to avoid detection. Destroying their presence is a crucial requirement for any intruder to avoid any detect back. This is achieved by deleting possible error messages received during the invasion on the network or system. For e.g., the buffer stack overflow error will leave a message that needs to be deleted in the system logs.

Tools used for clearing tasks

OS forensics

Opposing the current problem

Different organizations are working towards improving the concept of ethical hacking and how they can implement it better for future security.

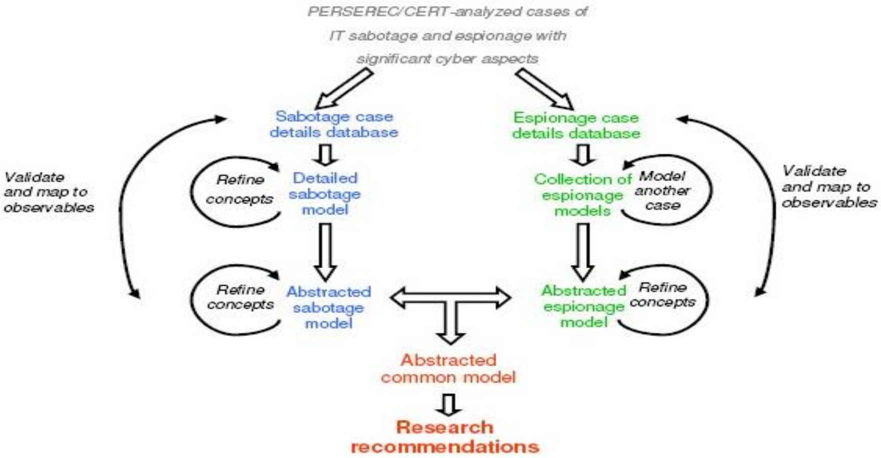
PERSEREC/CERT-analyzed cases of
IT sabotage and espionage with
significant cyber aspects
Sabotage case details database
Espionage case details database
Validate and map to observables
Refine concepts
Detailed sabotage model
Collection of espionage models
Model another case
Validate and map to observables
Refine concepts
Abstracted sabotage model
Abstracted espionage model
Refine concepts
Abstracted common model
Research recommendations

Figure 2: *Attack analysis [5]*

The model showed above **[5]** gives us relative information about the problem faced by the hacker and how they reduce its impact and minimize risk involved. One other method we can implement is the use of automate ethical hacking, but due to it been a machine it causes concerns as they can mismanage some information and crash due to any hardware or software related issue.

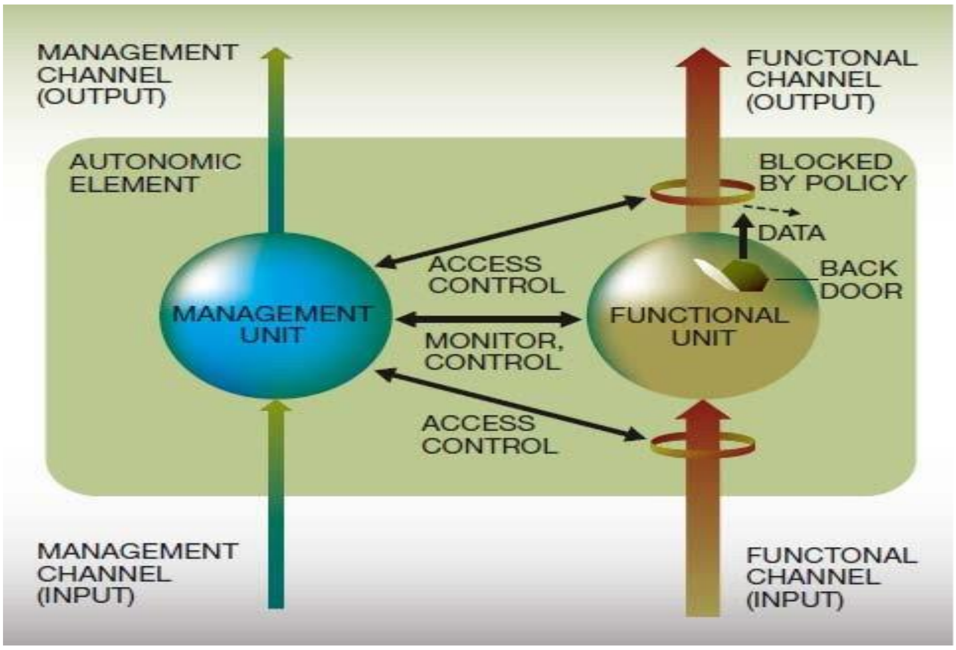

Figure 3: *blockage of back door by automatic system [6]*

Why it is necessary in our society

Continuously hackers are marking their influence on the younger generation of computer science enthusiasts, although ethical hacking has its merits, we should also know what these hackers are doing for our society and how we are benefiting from their contributions.

To save people from getting scammed and violating their privacy

Ethical hackers can save personal data of the client, many scammers use different software to infiltrate the system of the client and steal their confidential information which they later extort, these can be reduced if a business from which a client was affected by the hacker use penetration testing. Further improving their security and enhancing user experience.

How the younger audience is influenced

Hacking in itself is considered bad if one is miss using it, but students should be given up to date information about the IT and other related fields so they can differ and understand what is deem good and bad for society and how it affects the people in and outside this industry. A very big problem with undergraduate students to teach this approach that a teacher is effectively providing a loaded gun to them **[7]**.

Business needing ethical hackers

Nowadays every organization uses the implementation of IT. With this method we can ensure our data is available to everyone on the network electronically. Due to this fact it is easy for most hackers to steal confidential information. Any program or website has its flaws and some exploit these to their own benefit, so most businesses try to give rewards to individuals who give them feedback to these vulnerabilities present in their system or network. E.g., Companies like IBM employ teams of Ethical Hackers to keep their systems secure.

Impact on Technology

As everyone is aware information is widely available to everyone on the internet, they can use it for their own betterment, or some use it for malicious intent. Nmap a tool available on the internet that helps with information gathering on local or networked system. Ethical hackers can get access to the IP addresses of these network. Using Nmap can help an ethical hacker in their effort to reduce vulnerabilities, but since this technology has been used by any hacker it can be used for both good and bad. While a malicious hacker will use it for their own advantage, the ethical hacker will use it for their client's security and organizational benefits.

This further helps the growing industry to identify the loopholes in their network and improve their workplace confidentiality and customer's privacy.

Confidential information misuse

Confidential information is the most important aspect that ethical hacker focuses on, since most of the related hacks are focused to extort information and mis use it to gain profits, a recent report exposed that spam contributed to 70% of all the emails on the internet **[8].**

Conclusion

As technology will continue to grow, so will hacking. A hacker as stated can be ethical or unethical but it is our duty as creators of these magnificent technologies to improve the security and vulnerabilities so we can save ourselves from malicious intent.

We innovative every year by various means, but so do hackers they will find new ways to infiltrate the network system be it for good or bad intentions is up to them. But if it is possible security to improve in a way that we can differ the way hackers interact and differentiate between a good or bad hacker, it will benefit us from knowing which individual actually has good intentions for the client or organization.

References

Jon Erickson, 2008, "Hacking: The art of exploitation", 2nd Edition, No Starch Press Inc., ISBN-13: 978-1-59327-144-2, ISBN-10: 1-59327-144-1

Jamil, Danish, and Muhammad Numan Ali Khan. "Is ethical hacking ethical?." International Journal of Engineering Science and Technology 3.5 (2011): 3-758.

S. Patil, A. Jangra, M. Bhale, A. Raina, and P.Kulkarni, "Ethical hacking: The need for cyber security,'' in IEEE International Conference on Power, Control, Signals and instrumentation Engineering, ICPCSI 2017, 2018, doi: 10.1109/ICPCSI.2017.8391982.

P. Engebretson, "Reconnaissance," in the Basics of Hacking and Penetration Testing, 2011

S. Band, D. Cappelli, L. Fischer, AP. Moore, RF. Trzeciak and E. Shaw, "Comparing Insider IT Sabotage and Espionage: A Model- Based Analysis", Carnegie Mellon University, 2006.

D. M. Chess, C. C. Palmer, S. R. White, Security in an autonomic computing environment, IBM Systems journal, Vol 42, No 1, 2003

Tom Wulf, 2003, "Teaching Ethics in Undergraduate Network", Consortium for Computing Sciences in College, Vol 19 Issue 1, 2-3.

Ankit Fadia, 2005, "The Ethical Hacking: Guide to Corporate Security",1st Edition, ISBN: 989-615-004-4