Ethical hacking and penetration testing for securing us from Hackers

Pradeep I 1 and Sakthivel G 2

1 Department of Physics, Sri Krishna College of Engineering and Technology

2 Department of Mechanical Engineering, Sri Krishna College and Engineering Technology

E-mail: Pradeep@skcet.ac.in, sathishsakthi843@gmail.com

Abstract: Almost all the people around the world are fully equipped with technologies and software’s. But the how many are really using it wisely, we as the creators of all technologies are being governed by such a technology itself. The software’s are being discovered every day and each one provides a new facility and a hidden disadvantage in it. Many people don’t even have the basic knowledge of what they are doing and that’s the main reason for all cyber-crimes and security breaches. It has become responsibility of every citizen who is using a tech to keep their information safe and secure from others. Be aware of what we are doing in mobiles, laptops, PCs, etc.... since a small activity could lead to great crisis.
Introduction

In today’s World, Technology plays a major a role. We are evolving and moving in tech everyday also with the help of these technologies we have crossed many milestones. But have you ever taught how far these technologies can go? What are the limitations to these technologies? and what is happening in background when we really use such a technology?

Certainly not, many people don’t take care of this. It is much more important to be secure in every aspect we govern these technologies. And this following paper will help you to be safe in governing technologies.

Every technology which we are handling has a great advantage and unnoticeable disadvantage too. That is mainly used as loop holes by hackers and this leads to many crimes now a days.

1. Hacking

Getting access to server without the knowledge of the user. The server may be internet systems, personal computer, accessing main hub, etc... the person who is doing such an activity is termed as hacker. There are different types of Hackers around the world.

1.1 White hat hackers:

The person who can get access the systems and find the loop holes and mistakes in that particular systems, and make a report to the respective organization in order to rectify the errors in the system are named as White Hat Hacker. They can also be termed as Ethical Hackers.

1.2 Black hat hackers:

These are the persons who get access into the systems without knowing the organization or the user for stealing sensitive information such as account
details, photos, videos and even nuclear launch codes too. They are called as Black hat hackers.

1.3 Grey hat hackers:

These people will be on both sides, they will be accessing the systems for stealing information’s and at the same time they report to the organization for rewards. They are named as Grey Hat hackers.

1.4 Script kiddies:

They are just normal persons but they tend use the scripts and codes which are already designed by the professional hackers. In general, they don’t have the knowledge of hacking.

2. Be an Ethical Hacker

In order to get rid of the cyber-crimes and to make our self-safe from these crimes, we should know the some basic about the technology or software what we are using. It is not necessary to be a hacker to stop these activities. We should aware of what we are doing in our systems. If we want to be hacker, we should be an Ethical Hacker.

Ethical hacker always get access into the systems by getting permission from the user or organization. And found the loop holes in the systems and help the organization to resolve it.
3. Importance of Ethical Hacking

In the beginning of internet crimes such as terrorists seeks the help of hackers for breaching security systems, stealing sensitive information like nuclear launch codes or to extract huge amount of money form famous personalities by introducing a malware or spyware into their systems. Now it becomes great demand for every organization to be more defensive against such cyber-crimes.

Every day new types of viruses, malwares are being developed which raises the demand for Ethical Hackers to be more secure and safe from the cyber criminals and to safeguard our privacy information.

3.1 Information characteristics

Information is much more important in today’s world. Information reveals all privacy, security, and personal identity of an organization or an individual personality. Information is wealth. Some characteristics makes information more valuable. Such as

3.1.1 Confidential

It means that the information can be accessed only by authorized person. The main aim of confidentiality is to safe the sensitive information from cyber criminals. The privacy is usually maintained by Confidentiality. Example: Encryption.

3.1.2 Availability

The information which we are requesting should be available only for us. This provides us guarantee for accessing the information which we are seeking. We
should update all the source files and we should be ready with the recovery options in case of loss of data.

3.1.3 Integrity

This helps us to maintain the accuracy of information when it is transmitted, stored and processed. This acts as a basic firewall between you and unauthorized person. Examples: RSA signature, hash codes, etc.

3.1.4 Authentication

It is used for the verification of data, whether it is genuine or not. This feature allows only the authorized person could access the data for what he/she looks for.

Example: Asking for login credentials for particular websites.

4. Hacking Stages

4.1 Reconnaissance

It is the first stage in hacking. It is also known as information gathering or footprinting. It is a surprise to see that Google Chrome itself is vulnerable to footprinting. This is the stage where we used to collect all the details about the target system. The three groups of collecting information is Network, Host and People who is involved.

4.1.1 Types of footprinting

- **Active**: It involves direct interaction with the target system to collect the information. Example is using a Nmap tool.
• **Passive:** This involves collecting the information without interacting with the system directly.

4.2 **Scanning**

• **Port scanning:** It involves scanning for information like open ports and various services running on the target.
• **Network mapping:** This involves in finding the trace route of network, routers, firewalls and this helps the hacker to draw a map and which may provide valuable information for breaching.
• **Vulnerability scanning:** This scanning involves in finding all the vulnerabilities to get access into systems.

4.3 **Gaining access**

It’s a third stage of getting access from the target system. It can be done with the help of some tools or chronological methods. After getting access he should raise his position to administrator level so that he can modify the entire systems.

4.4 **Access Maintaining**

The person who involves in hacking the systems either for testing or for stealing will have to be in a position to keep hold the access that he/she has authorized. It can be done with some types of software’s and trojans. The ultimate aim is to maintain the access until the job is done.

4.5 **Track clearing**

All person those who are involving in crimes will always don’t want to caught up. A clever cyber attacker will always clear all the traces that leads the way to trace him.

Examples: modifying the activity logs, deleting the folders that he created.
5. Laws and standards

- The federal Information Security Management act (FISMA)
- The digital Millennium copyright Act (DMCA)
- Sarbanes Oxley attack
- HIPPA – Health Insurance Privacy Protection Act

6. Penetration testing

It is testing that looks for security loop holes to exploit. An advance penetration testing will look for all the loop holes and major issues in the systems. It may be security issue such as vulnerable to steal sensitive information. It is done usually a time dependent process and we cannot perform all the tests that we are thinking. Even if we have done all the tests for a particular software, it is said that the system is still not fully secured. It may be vulnerable to some more attacks. The best practice in penetration testing is that to set a time limit and set a priority to important tests.

*Types in penetration testing*

- **Black box** – The person who is penetrating will not be aware of any details that what they are penetrating in.
- **Grey box** – In this the tester will be provided with the minimal knowledge about the systems
- **White box** – The tester will be provided with all the knowledge of the systems to be tested.

7. Skills to be Ethical Hacker

Hacking into a system is like playing a game in a hard mode. The one who wish to Hack in an Ethical manner should be expert in coding and requires lot of
effort to be an Ethical Hacker. You need to be update with latest technologies and software’s.

An ethical hacker must be an expert in computer and needs lot of patience and determination to try again and again.

Also, to be an Ethical Hacker the person must clear Certified Ethical Hacker (CEH) Exam.

8. Safety tips to be protective

8.1 Strong passwords

Using different password combination and different username for various accounts such as Facebook, Instagram and various other websites will be protective. Ensure the password is tough to crack with combination of letters, numbers and special characters.

8.2 Firewall Activation

In cyber world, the frontline defense is firewall, they restrict the unrecognized connection between you and a cyber-criminal.

8.3 Antivirus software

This software helps us to check any unnoticed or hidden viruses, spyware or malware being introduced to our systems without our knowledge and helps to remove such malwares also.

Examples: k7 antivirus, Norton, etc.
8.4 Securing mobile devices

Our mobile devices which we are using is vulnerable to viruses and malware attacks. We should download each application from trustworthy sources.

8.5 Blocking spyware attacks

As said earlier we can block the spyware entering into our systems rather cleaning it after being intruded into us. Keep update antivirus software in order to achieve such protection.

8.6 Have latest version of operating system

We should always be in update with developing technologies and we should update our operating systems associated with their organizations to prevent form cyber-attacks.

8.7 Protect our information

We can separate protective methods such as turning on encryption for particular important files to be more protective from vulnerable attacks.

8.8 Be social media savvy

We should be in a position to set our profiles in private and we should be aware of the settings and privacy policy of each application that we are using in mobiles, PCs, etc. And be careful when you post something on your social media profile.

Conclusion

As the Technologies develops the drawbacks also develops along with the advantages. In today’s world even medical technology has many disadvantages. We will be monitored every time even by google. As said Earlier we should be aware of things what we are doing in software’s. And we should not allow the
technology to govern to us, as we are the creators of these technologies, we should be the person who governs the technology. As long as the Earth exists the technology will also be alive. We should be safe at many times in order to avoid security breaches.

References:

1. Thomas, Georg Charles Sturt University, School of Computing and Mathematics, *Issues of Implied Trust in Ethical Hacking*
2. Al-Saggaf Y, Burmeister, O.K, and Weckert J, 2015. *Reasons Behind Unethical Behaviour in the Australian Ict Workplace: An Empirical Investigation," Journal of Information, Communication & Ethics in Society (13:3/4), pp. 235-255.*
3. Thomas, G. A (2017) “An ethical hacker can help you beat a malicious one”, *The Conversation.*
4. Thomas G, Low G, Burmeister O (2018) “Who Was That Masked Man?”: System Penetrations—Friend or Foe? In: Prunckun H. (Eds) Cyber Weaponry. Advanced Sciences and Technologies for Security Applications. Springer, Cham
5. Tutzauer C, (n.d.) *The Role of Trust in the Successful Implementation of Information Systems.*
6. Verizon (2017). “Verizon Data Breach Investigations Report 2017”
7. Verizon (2018). “Verizon Data Breach Investigations Report 2018”
8. Mansfield-Devine, S (2017). *Hiring ethical hackers: the search for the right kinds of skills. Computer Fraud & Security, 2017(2), 15–20. doi:10.1016/s1361-3723(17)30016-7*
9. Conrad J, (2012). *Seeking help: the important role of ethical hackers. Network Security, 2012(8), 5–8. doi:10.1016/s1353-4858(12)70071-5*
10. Backof J. F, & Martin, C. L. (1991). *Historical perspectives: development of the codes of ethics in the legal, medical and accounting professions.* Journal of Business Ethics, 10(2), 99-110.

11. Cole E, (2002). *Hackers beware.* Sams Publishing

12. Conran B, 2014. "*Why You Shouldn’t Hire an Ethical Hacker,*" Security (51:3), Mar 2014

13. Gay J. R, (2012). *A Code of Conduct for Computer Forensic Investigators* (Doctoral dissertation, University of East London).

14. Graves K, (2010). *Certified Ethical Hacker Study Guide.* Wiley Publishing Inc, Indiana, USA

15. IBM. (2015). *IBM 2015 Cyber Security Intelligence Index.*

16. Identity Theft Resource Center (2017). “2017 – Breach Category Summary”. 