International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT21765

Ethical Hacking : Roles, Phases and Impact on various sectors of the Economy

Ch. Mary Pushpa, K.V.M Udaya Lakshmi, S. Hepsibha
Assistant Professor, Computer Science, St. Pious X Degree & PG College for Women,Hyderabad, TS, India

Article Info
Volume 7, Issue 6
Page Number: 38-43

Publication Issue :
November-December-2021

Article History
Accepted : 12 Nov 2021
Published : 21 Nov 2021

ABSTRACT

This paper will discuss the topic of ethical hacking, which is also called penetration testing. It starts by briefing about the ethical hacking introduction and its key protocols. It will further discuss the varied classifications of hacking and explain the causes for the swift rise in the cyber-crimes and their impact on socio-economic growth. The advantages and limitations of ethical hacking are also listed. It will further discuss the steps involved in ethical hacking, who is allowed to conduct ethical hacking, and its importance in order to reduce the effect of these attacks, penetration tests are highly required, to consider an acceptable solution for this task.

Results from the case study shows that there are negative impacts where the society suffers from cybercrimes and why the computer or networking tools are targeted for the crimes. Ethical hacking education can provide the future professionals to combat the future cyber security issues.

Keywords : Security, Ethical Hacking, Hackers and Intruders, Testing, Roles of Hackers

I. INTRODUCTION

The world constitutes people who are connected to each other through the internet for communication and the most important factor is when information is transferred from one end to other end causes harm so it is important to secure an individual online from varied threats on online (Hacking).

Hacking refers to accessing information using a computer by either password cracker software or any other technique to get the data. [1]This can be achieved by pointing the loop holes in the security of a computer. An individual who likes to work on programming or system completely but not theory based.

Hacker or intruders main targets of hacking are Financial Gain, Espionage,Venting anger at a company or organization, Terrorism, Just for fun, Show off, Hack other systems secretly, Notify many people their thought, Steal important information.

The process of Ethical hacking involves an authorized attempt to gain unauthorized access to a computer system, data, or application. Ethical hack involves replicating strategies and actions of malevolent attackers. So, this kind of approach helps to identify security vulnerabilities which can then be

resolved before a malicious attacker has the opportunity to abuse them.

Hacking experts follow four key protocol concepts:

- **To Stay legal**. Before accessing and performing a security assessment need to have proper approval.
- **To define the scope**. Determining the scope of the assessment so that the ethical hacker's work will remain officially authorized and within the organization's permitted boundaries.
- **Report vulnerabilities**. During the assessment process notify the organization of all vulnerabilities and provide remedy or advice for resolving these vulnerabilities.
- **To Respect sensitivity of data**. Depending on importance of data the ethical hackers may have to accept to a non-disclosure agreement to other terms and conditions required by the assessed organization.

Ethical hackers use their skills and knowledge to provide security and improve the technology of organizations. Essential services are provided to these organizations for vulnerabilities that lead to a security breach. Most of the cases with the organization's consent, the ethical hacker performs a re-test to check whether the vulnerabilities are completely sorted and resolved[2]. The Malicious intruders try to achieve unauthorized access to any kind of resource for financial gain or personal recognition. Some malicious hackers hack websites or crash backend servers for fun, reputation damage, or to cause financial loss.

II. CLASSIFICATION OF HACKERS

Hackers are broadly classified into 5 categories.

a) White hat hackers:

White hat hackers are also called Ethical Hackers who hack computers of corporate companies for any loop holes in their security. These hackers are paid for this job which is known as Penetrating Testing.

b) Black hat hackers:

The complete contrast of White Hat Hackers are Black Hat Hackers who mainly focus on harming them but don't take hacking jobs from companies. They interrupt the systems so as to access information targeting bank information, personal details, phone numbers.

c) Grey hat hackers:

They are the amalgam of white hat and grey hat hackers.

d) Crackers:

This category are of college students hack systems for fun and personal use.

e) Script-kiddie:

This category contains broader area of non technical people having knowledge on professional hacking tools.

Precautions to be taken after hacked

- Shutdown or turn off the system
- Separate the system from network
- To restore the system with the backup and recovery or to reinstall all the programs for secure purpose
- Connect the system to the network
- Highly recommended to give a call to police.

III. HACKING PHASES

Hacking Can Be done by Following These Five Phases:

Phase 1: Reconnaissance - can be active or passive:

In passive reconnaissance the information is gathered regarding the target without knowledge of

the targeted company (or individual). It could be done simply by searching information of the target on the internet or bribing an employee of the targeted company who will reveal and provide useful information to the hacker[3].

This process is also called "information gathering". In this approach, a hacker does not attack the system or network of the company to gather information.

- Foot Printing
- Whois lookup
- NS lookup
- IP lookup

The Phase 2 takes The Information Gathered In Phase 1 for examining The Network. Tools such as Port Scanners, Dialers Etc. are being Used by the Hacker tTo Gain Entry in the Company's System And Network.

- Scanning
- Port Scanning
- Network Scanning
- Fingerprinting
- Fire Walking

Phase 3: Owning the System

Phase 3 comes to the Real And Actual Hacking Phase. The Hacker takes the information and examines In the above Two Phases To Attack And Enter Into The Local Area Network (LAN, Either Wired Or Wireless), Local Pc Access, Internet Or Offline. This phase also known as "Owning The System".

- Gaining Access
- Password Attacks
- Social Engineering
- Viruses

Phase 4: Zombie System

The intruder, after gaining the access in the system or network, keeps that access for upcoming attacks by making changes in the system in such a way that other hackers or security personnel cannot then enter and access the attacked system. In such a situation, the owned system (mentioned in Phase 3) is then referred to as "Zombie System.This is called as Zombie system

- Maintaining Access
- Os BackDoors
- Clears Tracks

IV. HACKERS DO AFTER HACKING

- Patch Security hole
- The other hackers can't intrude
- Clear logs and hide themselves
- Install rootkit (backdoor)
- The intruder once attacked the system will be able to use the system at any point of time further
- It contains trojan virus, and so on

V. ETHICAL HACKING

Ethical hacking, which is also called as penetration testing or white-hat hacking. It involves the same tools, techniques and tricks that hackers use, but with one major difference is that Ethical hacking is legal.

- Performs almost the same activities but with owner's permission
- Breaking into the computer systems by the independent computer security Professionals.
- No damage to the target systems or stealing information.
- Assess the target systems security and report about the bugs found back to owners.

Required skills for Ethical Hacking

- Breakage of independent computer Professionals into the computer systems.
- No damage to the target systems or stealing the information.
- Assess the target systems security and report about the bugs found back to owners.
- Routers: knowledge of access control lists, routers and routing protocols[4]
- Mainframes : knowledge of mainframes
- Network Protocols: TCP/IP; how they can be functioned and manipulated.
- Project Management: planning, leading, organizing, and controlling a penetration testing team
- Install scanner program
- mscan, sscan, nmap
- Install exploit program
- Install denial of service program
- Use all of installed programs silently

Advantages of Ethical Hacking

- An evolving technique
- It helps us to think like a criminal(black hat, grey hat).
- Secure systems are created which are less prone to external attacks
- It gives us a chance of knowing the weak spots in the security of the systems [5]
- To help in detection of crimes done through the internet.
- Provides security to banking and financial establishments.
- Detection and prevention of cyber terrorism.
- Everything here depends upon the credibility of the ethical hacker.

Disadvantages of ethical hacking

- Its based on the trustworthiness of the ethical intruder
- Hiring professionals is expensive.
- This only provides us a summary of things in proceeding.
- Loss of sensitive information.
- Feeling secured ux`naware of the external attack

VI. THE ETHICAL HACKER WILL HAVE THE FOLLOWING JOB ROLES

- Information Security Analyst
- Security Analyst
- Certified Ethical Hacker (CEH)
- Ethical Hacker
- Security Consultant
- Information Security Manager
- Penetration Tester

VII. AVAILABLE CODES

Many kinds of ethics and conduct are available in the information security industry. Few of the codes are

- Australian Computer Society Code of Ethics
- CREST Code of Conduct
- EC-Council Code of Ethics
- Global Information Assurance Certification
- ISACA Code of Professional Ethics
- ISC2 Code of Ethics

VIII. ETHICAL HACKING IN GOVERNMENT ORGANISATIONS

Governments generally take personnel information and sensitive data of their citizens and attach it to several government related schemes.[6] This is a massive security breach as the government couldn't secure such sensitive data, the need for ethical hacking increased during the past many years. This is the reason why the government is appointing ethical hackers to detect malicious hackers before they start doing their bug bounty programs.

Laws in India generally don't concentrate on ethical hacking but consider hacking as a punishable offense. It has neutral status. Ethical hackers are appointed by various government organisations to find and fix certain vulnerabilities related to security. Certain organisations often offer certifications like Certified Network Defence Architect(CNDA) where such are designed for US Govt agencies and work for selected organisations and contractors. Organisations like Indian Cyber Army are a group of Ethical Hackers for various Government agencies, politicians, Research agencies who work for various security challenges in this present digital era.

There are certain academic qualifications to gain a job as an Ethical hacker in government sectors like post-graduation is a must along with a diploma or a certified course in ethical hacking from a reputed institution Even Government agencies should develop a methodology of checking their effectiveness of data and network constraints from time to time and take necessary actions like appointing expert hackers.

Ethical hackers render their services in areas such as

- Cyber terrorism and Terrorist attacks
- Virus attacks on Government websites
- Attacks on Civilians data fed in Government related scheme databases
- Security breaches in e-commerce system
- At core level Discover flaws in the system
- Test open ended modem systems which connect remotely to a network
- Areas which compromise with national security features
- Areas which require upgradation in their security features due to hacking problems

A new certified ethical hacker can expect a salary of nearly 3-5 lakhs per year. Experienced hackers or ethical hacking experts can expect a salary in a range of 10-20 lakhs. [7]A new set of Hacking professionals called white hat hackers and ethical hackers are gaining prominence nowadays. Government sector banks having faced the brunt many-a-times are hiring professional help to secure their networks.

IX. CASES OF CYBER CRIMES IN THE PAST YEARS

Amazon.com, Ebay.com, and Yahoo.com are the most effected internet sites in February 2000 where cyber terrorists hacked their websites and made changes in their existing coding. The damage caused by those attacks were so severe that they had shut down forcibly and started doing the damage control. It was due to the shut down that they were able to manage future break ins.[8]

Western Union branch of First Data Corp was attacked by an individual hacker where he stole nearly 15,700 credit card customers details in September 2000 and used for his individual purpose. This became possible due to security breaches which were left out and unprotected way of storing the files.

VIII. REFERENCES

[1]. Vinitha K. P(2018) Ethical Hacking. International Journal Of Engineering Research & Technology

[2]. Aman Gupta, Abhineet Anand–(2017) Ethical Hacking and Hacking Attacks.International Journal of Engineering and Computer Science

[3]. Sonali PatilEthical hacking: The need for cyber security(2017)IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)

[4]. Ethical Hacking: The Art of Manipulation Shehan Shetty(2019) International Journal of Advanced Scientific Research and Management

[5]. Ethical hanking:A technique to enhance information security Gurpreet K(2013). International journal of computer applications(3297: 2007),vol. 2,Issue 12

[6]. Kumar Utkarsh" System Security And Ethical Hacking"

[7]. https://www.researchgate.net/publication/228217113_Case_Studies_of_Cybercrime_and_its_Impact_on_Marketing_Activity_and_Shareholder_Value
[8]. C.Nagarani Ethical Hacking and its value to Security(2015) Volume 1V, Issue X Global Journal for Research Analysis
[9]. https://training.kenet.or.ke/images/a/a8/Ethical_Hacking_Final.pdf
[10]. http://viva-technology.org/New/Viva-Converge/stud3V3.pdf
[11]. https://www.researchgate.net/publication/228217113_Case_Studies_of_Cybercrime_and_its_Impact_on_Marketing_Activity_and_Shareholder_Value
[12]. https://www.ijert.org/ethical-hacking
[13]. https://www.worldwidejournals.com/global-journal-for-research-analysis-GJRA/article/ethical-hacking-and-its-value-to-security/Mzg4Mw==/?is=1

Cite this article as :

Ch. Mary Pushpa, K.V.M Udaya Lakshmi, S. Hepsibha, "Ethical Hacking : Roles, Phases and Impact on various sectors of the Economy", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 7 Issue 6, pp. 38-43, November-December 2021. Available at doi : https://doi.org/10.32628/CSEIT21765
Journal URL : https://ijsrcseit.com/CSEIT21765