International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048
Volume 6, Issue 1, pp 28-32, January-2022
https://doi.org/10.47001/IRJIET/2022.601007

Ethical Hacking: Types of Hackers, Cyber Attacks and Security

[1]Foram Gandhi, [2]Drashti Pansaniya, [3]Prof. Swapna Naik

[1,2]Student, Information Technology Department, Shri Bhagubhai Mafatlal Polytechnic, Mumbai, India
[3]Sr. Lecturer, Information Technology Department, Shri Bhagubhai Mafatlal Polytechnic, Mumbai, India

***Abstract* - This paper explores the ethics behind ethical hacking and the problems that lie with this emerging field of network security. The purpose of this paper is to tell what is hacking, who is hackers, what is ethical hacking, what is the code of conduct of ethical hackers and the need of them. Basically, hacking is the expertise in any field that can be used for both ethical and unethical purposes. Therefore, hackers are classified as per their working and as per their knowledge. The hackers are classified as white hat hackers, lack hat hackers and grey hat hackers. It focuses on the role of ethical hacker to remove it from the offender, Cyber-crime and illustrate on proactive approach to decrease the threat of hacking and Cyber crimes.**

Keywords: Ethical Hacking, Cyber Attacks, Security, White hat hacker, Black hat hacker, Grey hat hacker.

I. INTRODUCTION

In the world of cooperation, ethics take part an essential role for the employee and the employer. Ethics is a set of rules or concept that is regarded as standards, which are generally forced by a community or a profession.

Hacking is the illegal and unauthorized access to someone's private data or system. Hacking can be broadly divided into ethical and unethical hacking. Ethical hacking is a technique for securing and defending computer systems. Independent computer security professionals hack into a computer system without causing harm or stealing information. They assess the target system's security and notify the owner of any threats discovered.

Unethical Hacking significantly affects the development of systems and networks. An unethical hacker is carried out without the target's knowledge. Hacking without permission is illegal, and those who do it are considered cybercriminals.

Ethical Hacking can be defined as a legal access of an Internet geek or group in any organization's online property after their official permission. An ethical hacker attempts to bypass system security and search for any weak points that could be exploited by malicious hackers.

Ethical hackers are those who can build a firewall based on your skills and needs and secure all vulnerable points to prevent private data from being hacked. Hacking is not a criminal term; computer programmers refer to themselves as hackers because they can break into a device and solve problems. To overcome the risk of being hacked by the hackers we have Ethical Hackers in the industry, which are also computer experts just like the hackers but with good intensions or bounded by some set of rule and regulations by the various organizations. These are the persons who try to protect the online moving data by the various attacks of the hackers and keeping it safe with the owner.

II. TYPE OF HACKERS

Figure 1: The hackers' square measure categorized sales of Hackers

According to the ways of working or according to their intension, Hackers can be classified into three groups.

1. White HatHackers
2. Black HatHackers
3. Grey HatHackers

White Hat Hackers /Ethical Hacking

Ethical hacking is an information security branch and also called as "Penetration testing" or "White Hat hacking". They are waged professionals. To overcome the risk of being hacked by hackers, we have ethical hacker in this field, which are specialized in computer security that violates and find loopholes in protected networks or computer systems of some organizations or companies and corrects them to improve security working under set of rules and regulations by various organizations. These are the people who try to protect data while on the internet with various attacks from hackers and keep it safe with the owner. Ethical hackers use the same approaches as black hat hackers but their intention is to use

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 6, Issue 1, pp 28-32, January-2022

https://doi.org/10.47001/IRJIET/2022.601007

their knowledge productively. Information obtained from ethical hacking is used to maintain the security of the system and to prevent system from further potential attacks.

Black Hat Hackers

Cracker is the other name of Black hat Hackers. Crackers are highly skilled programmer's breaks into someone system has malicious intent to steal or destroy their important or confidential information or compromise the security of some institution, close or change the functions of sites and networks. Crack system security for personal gain is the main goal of cracker. These people generally demonstrate their extensive knowledge of computers and commit various cybercrimes, such as identity theft, credit card fraud etc. Student used his hacking skills to hijack webcams to catch young women pictures in various stages of undress (Humphries 2008). So, this act is considered as illegal hacking which is highly unethical and affecting the lives of the common people.

Grey Hat Hackers

A Gray Hat Hacker is a security expert who frequently breaches the law but has no malicious intent such as the black hat hackers. The word Gray Hat is obtained from Black Hat and White Hat because white hat hackers or ethical hacker discover weaknesses and loopholes in the networks and computer system or and do not tell anyone until it is fixed, while others hackers apart from the black hat illegally hack the computer system or the network to discover loopholes and leak the information to the third parties and the gray hat hacker does not illegally hack and does not tell anyone how to do it.

III. ADVANTAGES OF ETHICAL HACKING

While ethical hacking is a great role model into day's security era, where the number of people using networks is constantly growing. The hacker styles who take advantage of network benefits when remaining at home. The following are the key benefits of ethical hacking that have been established.

- Terrorism and defense challenges in the fight against terrorism.
- Preventing malicious hackers from gaining access to sensitive data.
- Ethical hackers believe that an individual can better secure the systems by causing minimal damage and ultimately fixing the discovered vulnerabilities.
- Ethical hackers use performance measures to apply their skills.
- This prevents identity theft and the leaking of vital information.
- It allows them to implement stronger security measures.
- It is also beneficial to help government entities to protect major computer system from being compromised in a way that national security would be an issue.
- Ethical hacking also helps families of deceased people to access account to see what their final vital transmissions may have been or gain access to some accounts to close them down.

IV. DISADVANTAGES OF ETHICAL HACKING

- This may corrupt the files or data of an organization.
- They might use information gained for malicious use. Subsequently, trustful programmers are expected to have achievement in this framework.
- By hiring such professionals will increase costs to the company.
- This technique can harm someone's privacy.
- The possibility that the ethical hacker will send and/or place malicious code, viruses, malware and other destructive and harmful things on a computer system.

V. PROCESS OF ETHICAL HACKING

The preplanning is arranged in various steps for performing ethical attack to the system security testing legally. All technical, management and strategic issues must be considered. Proper planning is very crucial for security testing from simple password security test to all high-level network penetration tests. Back up of data and information should be kept before committing ethical hacking. So, a well-defined scope involves the following information:

1. Specific systems to be tested.
2. Risks that are involved.
3. A proper test schedule is prepared overtime.
4. Use knowledge or experiences to explore security threats.
5. Assessment report of security for high level counter measures and start with most crucial cyber tests.

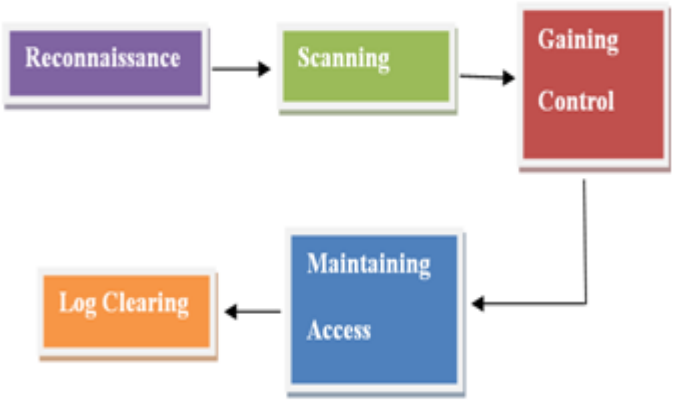

Figure 2: Process of Ethical hacking

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 6, Issue 1, pp 28-32, January-2022

https://doi.org/10.47001/IRJIET/2022.601007

Reconnaissance

The process of collecting information about the target system is called reconnaissance. The process includes finding vulnerabilities in the computer system, which means finding the ways which are left vulnerable. The further process of hacking is carried by the hacker if the hacker finds anyway to access the system. At the end of the reconnaissance phase the hacker has a bunch of information using which he can construct a promising attack on the target system.

Scanning

Before the attack hacker wants to know what system is up, what applications are used, what are versions of the applications. In scanning, searching of all open, as well as closed ports is done means finding a way to enter the system. It includes obtaining target's IP address, user accounts etc. In this phase the information gathered in the reconnaissance phase is used to examine the network and tools like Dialers, Port scanners etc. are used. Nmap is the popular, powerful and freely available tools used in scanning.

Gaining Control

This is the real part of the hacking procedure where the information gathered in the previous two phases is used to enter and take control of the target system through the network or physically. This phase is also called "Owning the System".

Maintaining Access

After gaining entry in the system in the previous step the hacker maintains the access to system for the future attacks and make changes in the system in such a way that any other security personal or any other hacker does not get the entry into the system into which is hacked. This is the situation in which the attacked system is known as the "Zombie System".

Log Clearing

It is the technique of removing any leftover log files or any other types of evidences on the hacked system from which the hacker can be caught. There are various tools in the ethical hacking techniques from which a hacker can be caught like penetration testing.

After reading about hacking and the shades of hackers there should be some way or some technique of protecting the computer system or the computer networks form the malicious hackers, therefore the terms "Ethical Hacking" and "Ethical Hackers" came into the industry.

Port Scanners	Nmap, Superscan, Unicornscan, Nikton, Angry IP Scanner, Auto scan.
Packet sniffers	Wireshark, TCPdump, Ethercap, EtherApe ,Dsniff.
Vulnerability Exploitation	Social Engineering ToolKit, Sqlmap, Sqlninja, BeEF, Dradis, Metasploit, Netsparker.
Vulnerability Scanners	Open VAS, QualysGuard, Nexpose.
Hacking Operating System	Krypton, SE Linux, Backbox Linux, Knoppix
Intrusion Detection Systems	Snort, NetCap

VI. COMMAN CYBER ATTACK

- Un-targeted Attacks.
- In un-targeted attacks, attackers randomly target as many devices, services or users as possible. They do not care about who the victim is as there will be a number of machines or services with weakness. To do this security issue they use techniques that take advantage of the openness of the Internet, which include:
- Phishing - sending emails to large numbers of people asking for sensitive information (such as bank details) or encouraging them to visit a fake website.
- Water holding-setting up a fake website or compromising a legitimate one in order to exploit visiting users.
- Ransomware - which could include disseminating disk encrypting extortion malware?
- Scanning - attacking wide swathes of the Internet at random.
- Targeted Attacks.
- Spear-phishing: sending emails to targeted individuals that could contain an attachment with malicious software or a link that downloads malicious software.
- Deploying a botnet: to deliver a DDOS (Distributed Denial of Service) attack.

VII. MITIGATING CYBER CRIME

Cybercrime is the use of a target's computers and information, particularly over the Internet, to cause physical harm or serious infrastructure disruption. Cybercrime, according to Kevin G. Coleman and colleagues, is described as "The intentional use or threat of destructive activities against computers and/or networks with the intent to inflict damage or further social, ideological, religious, political, or similar goals, or to threaten any individual in furtherance of such objectives."

Importance of Ethical Hacking and How to Minimize the Security Threats Ethical Hacker is the network and computer security professional who apply their knowledge and skills in defensive purpose. Roles of ethical are following:

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 6, Issue 1, pp 28-32, January-2022

https://doi.org/10.47001/IRJIET/2022.601007

- Assess the network and computer system's weak ties.
- Analyze the network traffic for malicious content.
- An ethical hacker serves as a network and computer system security advisor.
- Penetrating Testing should be avoided on the information system or network.
- Determine the system's security threat. Installing an advanced authentication or IDS system
- Prevents unauthorized access to a network or system.

VIII. CASE STUDY

Cosmos Bank Cyber Attack in Pune

A recent cyber attack in India in 2018 was deployed on Cosmos Bank in Pune. This daring attack shook the whole banking sector of India when hackers siphoned off Rs. 94.42 crores from Cosmos Cooperative Bank Ltd. in Pune. Hackers hacked into the bank's ATM server and took details of many visas and rupee debit cardholders. Money was wiped off while hacker gangs from around 28 countries immediately withdrew the amount as soon as they were informed.

Yahoo Data Breach

The Yahoo data breach broke all records of data theft in the history of cyber crimes. Yahoo found itself at the target point of hackers not once but twice as it came to terms with more than 3 billion user accounts being stolen! This incident put personal information such as name, phone number, email ID and passwords of 3 billion users out in the open! And the mystery continues till date as Yahoo struggles to find how this data breach was initiated and executed.

LinkedIn Hacking

Social networking website LinkedIn fell prey to a hack executed by Russian cyber criminals who stole the passwords of nearly 6.5 million user accounts. Soon these stolen passwords were made available in plain text on a Russian password forum! Adversity struck again when LinkedIn discovered in May 2016 that an additional 100 million compromised email addresses and passwords that were claimed to be from the 2012 breach, were released into the hacker forum. Some tech news reports have revealed that hackers were trying to sell this information on a darknet market for around $2200 each.

IX. HACKING TOOLS

Intruder

Intruder is a fully automated scanner that finds cyber security weaknesses in your digital estate, and explains the risks & helps with their remediation. It's a perfect addition to your arsenal of ethical hacking tools. With over 9,000 security checks available, Intruder makes enterprise-grade vulnerability scanning accessible to companies of all sizes. Its security checks include identifying misconfigurations, missing patches, and common web application issues such as SQL injection & cross-site scripting.

Nmap

Nmap is a security scanner, port scanner, as well as a network exploration tool. It is open source software and is available for free. It supports cross-platform. It can be used for network inventory, managing service upgrade schedules, and for monitoring host & service uptime. It can work for a single host as well as large networks. It provides binary packages for Linux, Windows, and Mac OS X.

Metasploit

Metasploit is an open-source pen-testing framework written in Ruby. It acts as a public resource for researching security vulnerabilities and developing code. This allows a network administrator to break into his own network to identify security risks and document which vulnerabilities need to be addressed first. It is also one of the few ethical hacking tools used by beginner hackers to practice their skills. It also allows you to replicate websites for phishing and other social engineering purposes.

X. CONCLUSION

The entire world is moving toward technological advancements and increasing digitization of real- world operations, which raises the risk of security. The workings of malicious hackers or crackers, on the one hand, who try to illegally break into security, and white hat hackers or ethical hackers, on the other hand, who try to preserve security, were identified in this paper. Ethical hacking is not a criminal activity but malicious unethical hacking is a computer crime or cyber-crime. The main goal of ethical hacking is to provide data and information security from being stolen and fraudulent use by malicious attackers. The concept of security and trust is very changeable because cyber threats can attack from any level of your organization.

REFERENCES

[1] Vinitha K. P, Ethical Hacking, Special Issue –2016.

[2] Prashant Kumar Gavel, Ramakant Prasad, Nainsy Rathore, Deepshikha Yadav, Ethical Hacking and Cyber Security against Cyber Attacks, January – June, 2020, Vol. 10: Issue1.

ISSN (online): 2581-3048
Volume 6, Issue 1, pp 28-32, January-2022
https://doi.org/10.47001/IRJIET/2022.601007

[3] Bhawana Sahare, Ankit Naik, Shashikala Khandey, Study of Ethical Hacking, Nov – Dec 2014, Volume 2 Issue 4.
[4] Mukesh. M, Dr. S. Vengateshkumar, Ethical Hacking, October 2019, Volume 3 Issue 6.
[5] K. Pavan Kumar, K. Pranathi, A Survey on Ethical Hacking, Approaches, Attacks, Procedure & Reliability incase of Cyber Crime, 16th April 2021, Volume 14, Issue 4.
[6] Nayab Akhtar, Sana Ghafoor, Overview of Ethical Issues such as Security, Confidentiality and Hacking in Software Engineering, June 2021.
[7] Aman Gupta, Abhineet Anand, Ethical Hacking and Hacking Attacks, April 2017, Volume 6, Issue 4.

Citation of this Article:

Foram Gandhi, Drashti Pansaniya, Prof. Swapna Naik, "Ethical Hacking: Types of Hackers, Cyber Attacks and Security", Published in *International Research Journal of Innovations in Engineering and Technology - IRJIET*, Volume 6, Issue 1, pp 28-32, January 2022. Article DOI https://doi.org/10.47001/IRJIET/2022.601007

****

