The Major Role of Ethical Hacking In Future Industrialization

Dr.Antony Cynthia[1], Sethuranga skanthan PT[2], Vinoth S[3]
[1]Assistant Professor, Dept of Computer applications
[2, 3]Dept of Computer applications
[1, 2] Sri Krishna Arts and Science college Coimbatore

Abstract- *In shaping the future of industrialization, ethical hacking, a crucial component of cyber security, will play a significant role. As industries migrate to the digital era, they are more vulnerable to cyber threats, which put operations, sensitive data, and even public safety in danger. White hat hackers also referred to as ethical hackers are crucial to the defense of these industrial systems. They develop strong defense strategies and proactively strengthen security measures by simulating cyber attacks and locating vulnerabilities. Additionally, ethical hacking helps industries uphold high ethical standards and protect customer trust by assisting in compliance with strict regulations. The importance of ethical hacking in securing vital infrastructure and cutting-edge technologies becomes paramount as automation, artificial intelligence, and the Internet of Things gain traction, fostering a safer, more resilient industrial landscape for businesses.[5]*

Keywords- Cyber attacks, Cyber security, Ethical hacking,

I. INTRODUCTION

As computer technology advances, so does its darker side: HACKERS. In today's world, the internet's size is rapidly expanding, and a large amount of data is moving online; thus, data security is a major concern. The internet has resulted in an increase in the digitization of various processes such as banking, online transactions, online money transfers, and online sending and receiving of various forms of data, raising the risk of data security. Nowadays, hackers target a large number of companies, organizations, banks, and websites with various types of hacking attacks. In general, when we hear the term "hacker," we think of bad guys who are computer experts with bad intentions and try to steal, leak, or destroy someone's confidential or valuable data without their knowledge.

There are computer experts who attempt to breach someone else's security in order to gain access to their personal information, but this is not always the case. To mitigate the risk of being hacked by hackers, the industry has Ethical Hackers, who are computer experts like hackers but with good intentions or bound by some set of rules and regulations imposed by various organizations. These are the people who try to protect online moving data from various hacker attacks and keep it safe with the owner. Furthermore, this paper informs you about hackers, ethical hackers, and the Linux operating system (Kali Linux), as well as some attacks carried out by hackers on the internet.[1]

II. WHAT IS HACKING?

Hacking is the technique of locating and exploiting weak links or loopholes in computer systems or networks in order to gain unauthorized access to data or change the features of the target computer systems or networks. Hacking is the modification of computer hardware, software, or networks to achieve goals that are not aligned with the user's goals. In contrast, it is also referred to as breaching someone's security and stealing personal or confidential data such as phone numbers, credit card details, addresses, online banking passwords, and so on.[1]

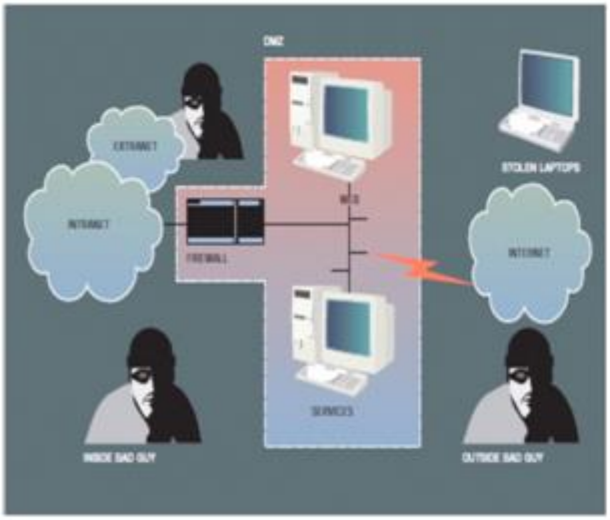

fig.1.Network

III. HACKERS METHODOLOGY

Reconnaissance:

Hacking is the technique of locating and exploiting weak links or loopholes in computer systems or networks in order to gain unauthorized access to data or change the features of the target computer systems or networks. Hacking is the modification of computer hardware, software, or networks to achieve goals that are not aligned with the user's goals. In contrast, it is also referred to as breaching someone's security and stealing personal or confidential data such as phone numbers, credit card details, addresses, online banking passwords, and so on.

Scanning: -

Before launching an attack, the hacker wants to know whether the system is operational, what applications are in use, and what versions of those applications are in use. Scanners search all open and closed ports in the hopes of finding a way into the system. It entails obtaining the target's IP address, user accounts, and so on. The information gathered during the reconnaissance phase is used to examine the network in this phase, and tools such as dialers, port scanners, and so on are used. and Nmap is a popular, powerful, and freely available scanning tool.

*Gaining Control***:-**

This is the actual hacking procedure, in which the information gathered in the previous two phases is used to gain access to and control of the target system via the network or physically.

Maintaining Access: -

After gaining access to the system in the previous step, the hacker keeps access to the system for future attacks and makes changes to the system so that any other security personnel or hacker does not gain access to the hacked system. In this case, the attacked system is referred to as the "Zombie System."

Log Clearing: -

It is the method of removing any remaining log files or other types of evidence on the hacked system from which the hacker can be identified. There are various tools in ethical hacking techniques that can be used to catch a hacker, such as penetration testing.[1]

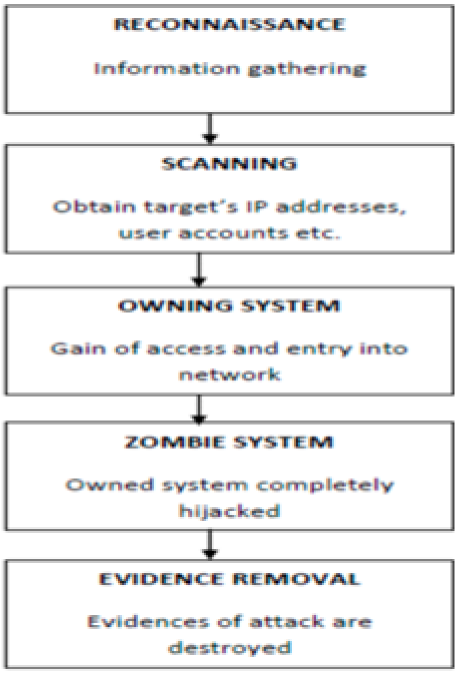
RECONNAISSANCE
Information gathering
SCANNING
Obtain target's IP addresses, user accounts etc.
OWNING SYSTEM
Gain of access and entry into network
ZOMBIE SYSTEM
Owned system completely hijacked
EVIDENCE REMOVAL
Evidences of attack are destroyed

fig.2. Path of hacking

IV. TOOLS USED BY HACKERS

The following tools are frequently used by computer criminals to enter networks:

- **Trojan horses:** are malicious programs or genuine software that are used to create a secondary entrance in a computer system so that a criminal can gain access.
- **Virus:** A self-replicating program known as a virus spread by inserting copies of itself into other executable code or archives.
- **Worm:** A self-replicating program, worms are similar to viruses. A virus appends itself to other code, whereas a worm does not. This is the difference between the two.
- **Vulnerability scanner:** Hackers and intruders use this tool to quickly scan computers on a network for known security flaws. Port scanners are also employed by hackers. This checks the ports on a certain computer to see if they are "open" or accessible to access the computer.
- **Sniffer:** This program intercepts watchwords and other data as it travels through the computer or over a network.
- **Exploit:** This is a program that takes advantage of a flaw that is already known.
- **Social engineering:** Using this technique, data can be obtained.

- **Root Kit:** This tool is used to hide how a computer's security has been compromised.[6]

V. ADVANTAGE AND DISADVANTAGE

Advantage:

- This prevents identity theft and the disclosure of sensitive information.
- It enables them to implement more stringent security measures.
- It is also advantageous to assist government entities in preventing major computer systems from being compromised in such a way that national security is jeopardized.
- Ethical hacking can also help families of deceased people gain access to accounts in order to determine what their last vital transmissions were or to close accounts.

Disadvantage:

- This may corrupt an organization’s files.
- The fundamental issue here is the trustworthiness of the ethical hacker.
- An ethical hacker could misuse the information.

VI. HACKING'S IMPACT ON BUSINESSES AND GOVERNMENTS

Businesses bear the brunt of extensive and costly hacking incidents, often becoming prime targets for hackers seeking customers' personal and financial data. These attacks can even originate from within the company, involving disgruntled or opportunistic employees. The financial repercussions are staggering; with yearly losses reaching billions of dollars, and the true impact may persist long after the initial breach. Such security breaches can lead to a loss of consumer trust and potential legal liabilities for the affected companies. Recovering from an attack entails various expenses, including legal fees, investigations, stock performance setbacks, reputation management, and customer support.

To prevent future attacks, businesses, and even consumers, are increasingly investing substantial amounts in pre-emptive security measures. Especially, companies handling large volumes of consumer data take additional precautions to ensure its protection. For example, Microsoft's MSN/Windows Live requires explicit consent from an internal security group before storing personally identifiable information.

Businesses lacking technical expertise often seek assistance from external security experts to bolster their defenses. ScanAlert.com is one such service, working with over 75,000 secure e-commerce sites, providing a "Hacker Safe" logo to signify daily security testing and a claimed 99.9% effectiveness against hacker crimes. However, it is crucial to note that this certification does not guarantee absolute security.

Scan Alert’s disclaimer acknowledges limitations, stating that the certification only indicates adherence to payment card industry guidelines for remote web server vulnerability testing. It cannot protect data shared with other uncertified servers or safeguard against non-hacker insider access. While scan alert makes reasonable efforts to ensure the certification's functionality, it disclaims any warranty or claim regarding the information's accuracy or usefulness. Users who access this information agree to hold scan Alert harmless in any event.[2]

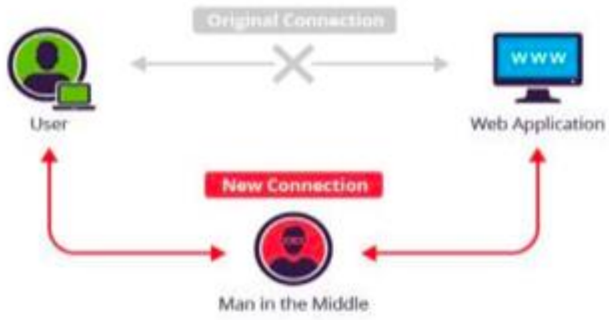

fig.3.connections

Ethical Hackers Are Required In The Industry

As each organization has its own confidential information that can be hacked or damaged by malicious hackers, the organizations’ ethical hackers must be allowed to hack their own systems ethically in order to find flaws or loopholes in their systems and correct them before any hacker hacks it.[1]

VII. PART OF ETHICAL HACKERS IN FUTURE INDUSTRIALISATION

Ethical hacking plays a vital role in the future of industrialisation by ensuring the security and resilience of modern industrial systems and critical infrastructure. As industries become increasingly reliant on digital technologies, networks, and interconnected devices, the risks of cyber threats and attacks also grow. Ethical hacking, also known as penetration testing or white-hat hacking, involves simulating cyber attacks on systems and networks to discover vulnerabilities and weaknesses before malicious hackers can exploit them.

The major roles of ethical hacking in future industrialization are as follows:

1. Enhancing Cyber security Assurance: Ethical hacking assists industries in evaluating the effectiveness of their cyber security measures. By proactively identifying vulnerabilities and potential entry points, organisations can take appropriate steps to address weaknesses and minimise the risk of successful cyber attacks.

2. Securing Critical Infrastructure: Industries like energy, transportation, healthcare, and manufacturing heavily rely on interconnected systems. Ethical hackers can assess the security of these critical infrastructures, preventing potential cyber threats that could lead to significant disruptions and damages.

3. Minimising Financial Losses: Cyber attacks can result in substantial financial losses due to data breaches, system downtime, and repetitional damage. Ethical hacking helps reduce these losses by identifying and addressing vulnerabilities before attackers can exploit them.

4. Ensuring Data Privacy and Compliance: With the increasing focus on data privacy regulations and compliance standards, ethical hacking helps industries identify weaknesses in data handling processes. This enables organisations to protect sensitive data, maintain compliance, and build trust with customers and stakeholders.

5. Protecting Intellectual Property: For industries reliant on research, development, and intellectual property, ethical hacking helps safeguard valuable assets from theft or compromise by malicious actors.

6. Supporting Secure Innovation: As industries adopt emerging technologies like the Internet of Things (IoT), artificial intelligence (AI), and cloud computing, ethical hacking provides the confidence to innovate securely. It helps identify the risks associated with these technologies and implement robust security measures.

7. Assisting Incident Response and Recovery: Ethical hacking is not solely about prevention; it also aids in incident response and recovery. In the case of a cyber incident or data breach, ethical hackers can provide valuable insights to understand the extent of the breach, identify its root cause, and support the recovery process.

8. Building Customer Trust: In an increasingly digital and interconnected world, customers expect businesses to protect their data and privacy. Ethical hacking demonstrates a proactive approach to security, which can enhance customer trust and loyalty.

9. Securing Supply Chains: Industrialisation involves complex supply chains with multiple partners and vendors. Ethical hacking can help assess the security posture of these supply chain partners, ensuring that potential weaknesses in the ecosystem are identified and addressed. [4][5]

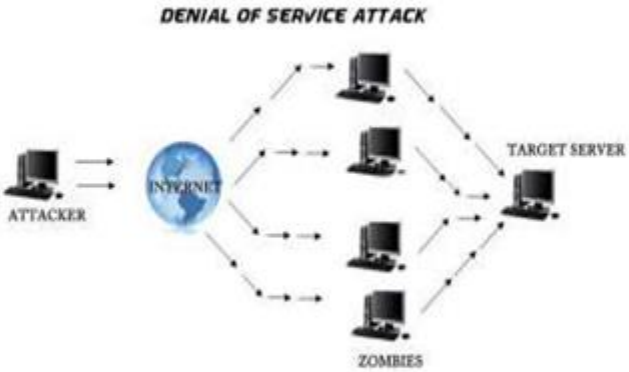

fig.4. denial of service attack

VIII. THE INDUSTRIAL CLOUD AND CLOUD SECURITY

Modern industrialization is not complete without cloud security and industrial cloud computing, which provide scalability, efficiency, and flexibility. However, this paradigm shift brings about particular cyber security difficulties that demand strategic defenses like ethical hacking. Adoption of the industrial cloud raises issues such as network vulnerabilities, unwanted access, and data breaches. A crucial part of discovering these risks and defending cloud systems is ethical hacking.

The protection of data integrity through encryption, effective Identity and Access Management (IAM) for controlling user access, and network configuration analysis are important considerations. Exploring potential flaws through vulnerability assessment and penetration testing (VAPT) encourages cooperation between ethical hackers and cloud providers for efficient correction.

For industrial cloud security, incident response plans and compliance observance are essential. Rapid threat identification and mitigation are made possible by cloud forensics and monitoring tools. It's crucial to embrace new trends as technology develops, such as zero-trust architecture and AI-driven security.

Real-world success stories demonstrate ethical hacking's value by exposing flaws that might have allowed breaches. Finally, ethical hacking contributes to overall security and increases public confidence in the digital transformation of companies by acting as a proactive defense in industrial cloud computing.[7]

IX. CONCLUSION

Hacking encompasses both advantages and risks, with hackers exhibiting a wide range of intentions and actions. On the one hand, they may cause financial harm to a company or, conversely, protect valuable data, leading to increased revenues. The ongoing conflict between ethical or white-hat hackers, who assist in understanding security needs, and malicious or black hat hackers, who illegally intrude for personal gain, seems never-ending. While ethical hackers play a crucial role in uncovering hidden vulnerabilities within servers and corporate networks, malicious hackers pose a significant threat by exploiting weaknesses in security systems.

Ethical hacking, when used appropriately, serves as a valuable tool to identify network weaknesses and potential exploits. It underscores the dual nature of hacking in the computer world, encompassing both constructive and destructive aspects. Ethical hacking serves a vital purpose in safeguarding sensitive information, while malicious hacking can lead to devastating consequences. Ultimately, the hacker's intentions determine the outcome. Though it may be challenging to bridge the gap between ethical and malicious hacking due to the complexities of human nature, implementing stringent security measures can help mitigate the risks associated with hacking.[2]

REFERENCES

[1] Aman Gupta, Abhineet Anand- Ethical Hacking and Hacking Attacks, International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 6 Issue 4 April 2017.

[2] Bhawana Sahare, Ankit Naik, Shashikala Khandey- Study Of Ethical Hacking, International Journal of Computer Science Trends and Technology (IJCST) – Volume 2 Issue 6, Nov-Dec 2014 .

[3] Vinitha K. P -Ethical Hacking ,International Journal of Engineering Research & Technology (IJERT) -ISSN: 2278-0181 NSDMCC - 2015 Conference Proceedings.

[4] http://searchsecurity.techtarget.com/

[5] http://www.wikipedia.org/wiki/ethical hacking

[6] Dr. Sunil Kumar , Dilip Agarwal - Hacking Attacks, Methods, Techniques And Their Protection Measures ISSN [ONLINE]: 2395-1052

[7] J. Danish and A. N. Muhammad, “Is Ethical Hacking Ethical?“ , International journal of Engineering Science and Technology, Vol 3 No. 5, pp. 3758-3763, May 2011.