Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X
Volume 4, Issue 2, 2026

CYBER SECUTIRY: IMPORTANCE OF WHITE HAT HACKER IN DIGITAL ERA

Waqas Ahmad[1], Uzair Iqbal[2], Muhammad Hamza[3]
[1]*CS & IT Department, Sarhad University, Peshawar*
[2]*Computer System Engineering, UET, Peshawar*
[3]*CS & IT Department, Iqra University, Peshawar*
[1]ahmadwaqas186@gmail.com, [2]engr.uzairiqba@gmail.com, [3]hamzawan012@hmail.com

DOI:

Keywords:
Hacking, Cyber Security, Ethical Hacker, Cyberattacks, Types of Hackers

Article History
Received on 10 Jan, 2026
Accepted on 07 Feb, 2026
Published on 08 Feb, 2026

Copyright @Author
Corresponding Author:

Abstract

Due to rapid development and advancement in Technologies in this digital era. The main goal of this study is to analyses the types of hackers and cyberattacks in the any organization. For this Purposes In the research paper wo focus on different types of hackers and their aim to hacked any system. There are two types of hackers. The first type includes those who act responsibly and ethically to enhance the safety of people and organizations. These are often called white hat hackers, red team, blue team, green team, and nation-sponsored hackers. The second type consists of hackers who use cyberattacks with harmful intentions, causing significant damage to public and private organizations and consumers. Furthermore, another part of this study to differentiate between ethical hacker and unethical hacker. What is his objection while hacked any system what type of tool and techniques are used by these hackers. also highlighted the importance of white hat hacker in an organization along with the limitation of these hacker.

INTRODUCTION

The practice of protecting data, systems, networks & devices from digital attacks is known as cyber security. The key concepts of cyber security are confidentiality, integrity, availability, and Authentication. Confidentiality in terms of cyber security is ensuring the information / Data is accessible to those users/ persons who are authorized to access that data. Integrity means data protection from altering and tempering by someone who's not authorized for access and modification. Availability means that information/data is available at any time when needed for only authorized users. While Authentication means verified user accessing the system/data/information.

The most important and valuable invention of the 21st century is the internet which has a great effect on the modern digital world. In this modern digital era, every communicating device is connected through the internet, and in terms of cyber security if a device is connected to the internet its security may be compromised and it can be easily hacked by hackers.

Nowadays, the internet has crossed every barrier to change the way we live in this world from shopping to payment all are done online which makes life easy in the current century. According to [1] a malicious code was written in the 1990's to damage/ harm the host computer by deleting important data/ information or appending it is known as a virus. Which also a type of cyber-attack through a system that helps with this malicious code (virus) because the modified file can damage the host system by an unauthorized person. This malicious code can spread through email, PIN drives, digital image audio files, or video clips. But the most important thing is that self-virus cannot affect the system it requires human interaction. Another class of virus is a worm which can replicate itself but it's different from a virus because it does not require a human interaction to activate.

Data security and privacy are some of the top precautions that are taken by organizations. Right now, we are living in a world where every piece of information/data is kept updated digitally or online [2]. Moreover, cyber security is a major concern nowadays in this digital era. The sharing of confidential data through the internet from source to destination means it is not secure and visible to hackers on the web to the outside world. Hacking creates fear and for that fear, several laws were implemented as well and many security measures were taken white hat hackers are one of them [3]. The work of a white hat hacker is the same as other hackers but that one is hired by the organization to check the variabilities of their system and to secure the system from outside attacks. It has access to the entire system to secure them and check the variabilities in them. White hat hackers are also known as ethical hackers and they work within the boundaries of law and follow these laws.

Cyber-attacks in Pakistan

Attack in Pakistan from 2020 to 2024 In the mentioned period three major attacks faced by Pakistan included spyware attacks, Financial Malware attacks, and industry control attacks. Below Figure 1.1 shows the number of attacks in this mentioned period.

According to (The Express Tribune) In Jan 2024 spyware attacks increased up to 300% from the previous year 2023. 114% year-on-year increase in Financial Malware attacks (Profile of Pakistan) while in the third quarter of 2024 29.51% increase in industry control attacks (pro-Pakistani).

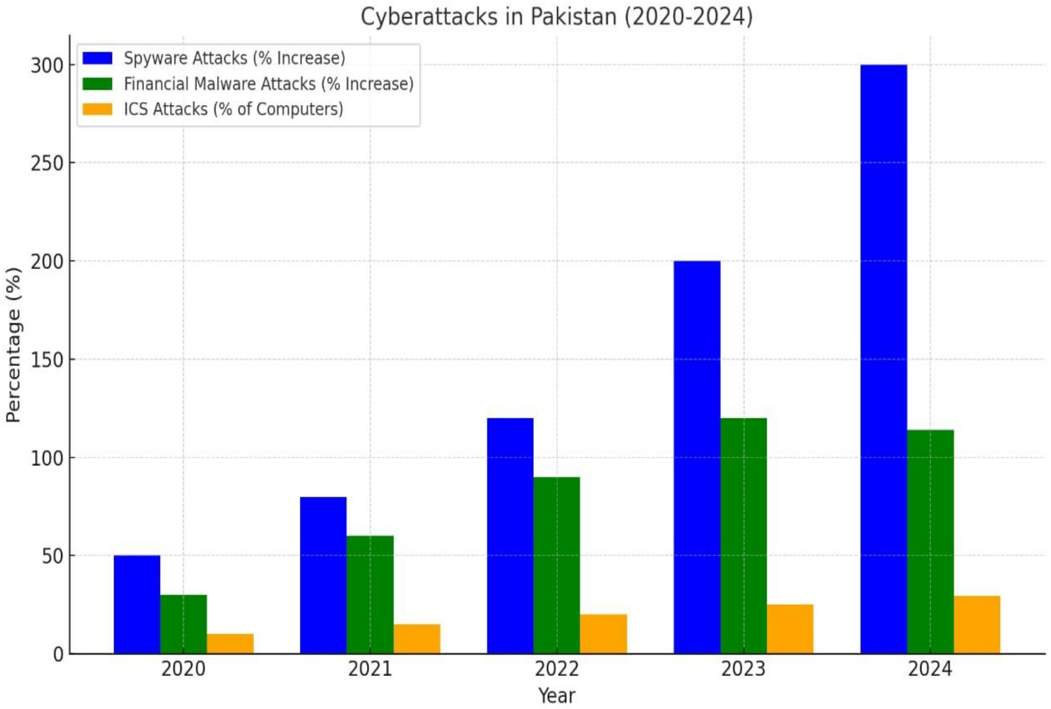

Figure 1 Attack in Pakistan from 2020 to 2024

Difference between Cyber-crime, Cyber-attacks, and Cyber-warfare

Feature	Cybercrime	Cyberattack	Cyberwarfare
Motivation	Primarily financial gain	Financial gain, political activism, espionage, sabotage, revenge	Political or military objectives
Targets	Individuals, businesses, organizations	Individuals, businesses, organizations, critical infrastructure	Critical infrastructure, military systems, government networks
Methods	Phishing, ransomware, malware, identity theft	Malware, denial-of-service attacks, SQL injection, social engineering	Sophisticated malware, zero-day exploits, advanced persistent threats
Impact	Financial losses, data breaches, reputational damage	Disruption of services, data breaches, system damage	Large-scale disruption, economic damage, loss of life
Attribution	Often difficult to attribute	Can be challenging, sometimes attributed	Often attributed to nation-states
Scale & Sophistication	Lowest	Moderate	Highest
Examples	Stealing bank account credentials, distributing ransomware	Hacking a website, stealing data from a company	Disrupting a power grid, attacking military systems

Table 1 Difference between cyber-crime, cyber-attacks, and cyber-warfare

Types of Cyberattacks:

1. Malware Attacks
2. Denial-of-Service Attack
3. Mian in the middle attack
4. Phishing Attacks
5. SQL Injection attacks
6. DNS spoofing
7. Trojan horses
8. Business Email Compromise (BEC)

1. MALWARE ATTACKS

Malware attacks are a common attack in cyber security in which malicious software is installed in a user system without the user's concern. Ransomware and spyware are common types of malware attacks. Bind the malicious code with the legitimate code, executed by themselves in a hidden location in the user system. Nowadays, the aim of malware is more on business or financial information than any personal credential information. The most common types of Malwares shown in table 1.2 [4]

Malware Type	Description	Key Characteristics	Spread Method	Potential Impact
Virus	Malicious code that attaches to programs and replicates.	Modifies code, self-replicating.	Executing infected files/programs.	Data corruption, system instability.
Worm	Self-replicating program that spreads across networks.	Independent, spreads without host program.	Email attachments, network vulnerabilities.	Denial-of-service, network congestion.
Trojan	Malicious code disguised as a legitimate program.	Hides within useful software, does not replicate.	Downloaded software, social engineering.	Data theft, backdoor access.
Ransomware	Locks user data and demands payment for its release.	Encrypts files, holds data hostage.	Various methods (e.g., phishing, exploits).	Data loss, financial extortion.
Spyware	Secretly monitors user activity and transmits data to attackers.	Operates covertly, collects user information.	Software downloads, website vulnerabilities.	Privacy violation, data theft.

Table 2 The most common types of Malwares

2. DENIAL-OF-SERVICE ATTACK

A denial-of-service attack overwhelms a system's resources, preventing it from responding to legitimate service requests. In a Distributed Denial-of-Service attack, multiple compromised machines, often controlled by an attacker, launch the attack. These attacks render the target machine or network resources unavailable to intended users by disrupting the service of the host connected to the internet.

Common types of DoS and DDoS attacks include TCP SYN floods, teardrop attacks, smurf attacks, ping-of-death attacks, and botnets. However, it becomes challenging to stop DoS attacks because legitimate and malicious traffic appears to be coming from the same ports and utilizing the same protocols.

Appropriate security measures would mitigate the risks of DoS attacks. In this regard, IDS and DDoS protection products are put in place. Ensuring the bandwidth on an internet connection to a particular organization can also be a means to mitigate low-scale DDoS attacks, providing for enough capacity of legitimate service requests. [4]

3. MAN-IN-THE-MIDDLE (MITM) ATTACK

A Man-in-the-Middle (MitM) attack occurs when an attacker intercepts communication between two parties. This allows the attacker to eavesdrop on messages, modify data, or even impersonate one of the parties. This type of attack poses significant risks, including unauthorized access to sensitive information and the ability to alter or manipulate data before it reaches its intended destination. [5]

4. PHISHING ATTACKS

Phishing is a social engineering tactic where attackers deceive individuals into revealing personal information through various methods, such as emails or fraudulent websites. The term originated in the 1990s and has evolved significantly since then, with attackers constantly devising new techniques. While the overall rate of generic phishing emails may have decreased, spear phishing remains a prevalent threat, often used to distribute malware. Despite efforts to combat phishing, the increasing use of HTTPS in phishing sites highlights the need for continued vigilance and robust security measures to protect against these evolving attacks. [6]

5. SQL INJECTION ATTACK

SQL Injection (SQLi) is an attack that takes advantage of vulnerabilities in the code of an application to inject malicious SQL code. It enables attackers to manipulate the database and gain unauthorized access to sensitive information, such as confidential organizational data or user details. SQLi attacks can have serious consequences, including unauthorized viewing or deletion of data and complete database compromise.

Attackers executing SQL injection, in fact alter the standard queries of SQL while attempting to compromise vulnerabilities in lightly protected databases. They will also use an unfiltered inclusion of special characters that change their SQL commands; however, preventing and protecting an attack is entirely possible.

Common of these is input validation. The method here calls for writing some checking code that rejects user inputs as inappropriate. However, this is really tough because no one can try to map out all the possibilities in legal and illegal inputs.

A better solution is the use of Web Application Firewalls. WAFs are able to filter malicious traffic very effectively, block SQL injection attempts with very low false positives, and therefore help reduce the risk of falling prey to SQL injection attacks for an organization by implementing a combination of input validation and WAFs. [4]

6. DNS SPOOFING

DNS Spoofing, also known as Domain Name System Spoofing, is a cyber attack that targets the Domain Name System (DNS) to redirect internet traffic.

The DNS is the foundation of the internet's infrastructure. It translates user-friendly domain names (like www.example.com) into numerical IP addresses that computers can understand. DNS spoofing exploits vulnerabilities in the process of resolving DNS queries. In a successful attack, attackers trick computers into associating a legitimate domain name with a false IP address. This manipulation can direct users to malicious or unwanted websites.

An alternative way to perform DNS spoofing is by exploiting vulnerabilities in a DNS server and injecting false data into its cache. This malicious practice is known as cache poisoning. A worrying third of all DNS servers on the internet are susceptible to spoofing attacks, according to the most recent "Domain Health Survey" (February 2003). These attacks can have major security repercussions for vulnerable DNS servers, such as misrouting emails or directing users to malicious websites. [Spoofing Attacks of Domain Name System Internet] [8].

7. BUSINESS EMAIL COMPROMISE

Business Email Compromise (BEC) is a sophisticated cybercrime where attackers impersonate trusted individuals or organizations to deceive victims into transferring funds or divulging sensitive information. BEC attacks often involve urgent requests, with 85% demanding immediate action. These requests commonly seek assistance (59%) or pertain to supply chain matters (26%).

BEC is a targeted attack aimed at businesses that frequently engage in financial transactions. Attackers exploit social engineering techniques by sending malicious emails that appear to originate from legitimate sources within the company, such as CEOs or CFOs.

The attack typically follows a methodical approach. Attackers meticulously research their target organization, gathering information from public sources like social media and making calls to establish rapport. They then focus on building trust with a specific employee who has access to company finances. This trust-building phase can take weeks or even months.

Once trust is established, the attacker executes the attack. They send an urgent request for a significant fund transfer, often mirroring typical transaction amounts to avoid suspicion. The request may include a fabricated excuse, such as the sender being unavailable due to a meeting or travel. The attacker then instructs the victim to transfer the funds to a controlled account, often located in another country.

BEC attacks often go undetected for some time, allowing the attacker to successfully transfer and control the stolen funds before the company realizes it has been compromised. [7]

9. TROJAN HORSES

Trojan horses are a significant threat to network security, functioning as a type of malicious software. While broadly categorized as viruses, Trojans exhibit distinct characteristics.

Firstly, Trojans possess strong concealment capabilities. Once successfully installed, they employ sophisticated hiding mechanisms to evade detection by the user, making complete eradication challenging.

Secondly, Trojans essentially act as unauthorized remote monitoring programs. They enable attackers to control and access the target computer without the legitimate user's consent, a defining characteristic of Trojan malware.

Finally, like other malicious programs, Trojans aim to spread. They often attempt to infect other computers, expanding their reach and impact within a network. [9]

EARLY BEGINNINGS OF ETHICAL HACKING

The early days of computing the concept of ethical hacking can be traced in 1960’s and 1970’s when the computer system became more frequent at that time the need of security measure grew. The word hacker originally refers to individual who gain the access of host system with the permission or without the permission of user. After that the concept of white hat and black hat hacker will generated. This exploration was frequently conducted without malicious intent, with the goal of improving system functionality and security.

As compared to This exploration was frequently conducted with malicious intent, with the goal of his personal intent.

MODERN DEVELOPMENTS

In recent years, ethical hacking has become widely recognized as a critical component of cybersecurity. Organizations from numerous industries now hire ethical hackers to undertake regular security checks. The advent of new tools and methodologies, such as automated vulnerability scanners and artificial intelligence-driven analysis, has increased the effectiveness of ethical hacking.

HACKING:

A malicious activity performs by a person for gaining access of host system to Explode the Vernability and weakness of the system for self and for explode sensitive information. In other word gaining of un unwanted access of system to get sensitive information/ data without authorization of host. Some malicious software was used like spyware. Trogen and malware to gain entry into the system or network for stealing vital in formation.

Identity theft, loss of private information, decreased productivity, misuse of network resources (e.g., bandwidth abuse and spam), illegal use of credit or debit card numbers, and the sale of user personal information (e.g., phone numbers, addresses, account numbers, etc.) are all possible outcomes. However, the practice is known as "Ethical Hacking" when the hacker has explicit plans to breach a computer system in order to protect the company against intrusion attacks. [10]

CLASSIFICATION OF HACKERS

Hackers can be classified broadly into three different categories:

1. Black Hat Hacker
2. White Hat Hacker
3. Grey Hat Hacker

1. BLACK HAT HACKER

Security Hacker or Unethical hacker are the other Names of Black Hat Hacker. These people hacked the system for stealing money or to achieved their own illegal goals. These types of hackers find the banks or organization with weak system Security for hacking their system or stealing other information about that organization. They also modified the system data or to destroyed the data that's way Black Hat hacking is illegal.

2. WHITE HAT HACKER

Penetration testing or Ethical Hacker are also known as White Hat Hacker. White hat hacker uses same techniques and software's as black hat hacker used. White Hat hacker hacked those system which they have permission to hack it for the purposes of security checking also checking the weakness of that organization / system. They focus on security and protecting IT system.

3. GREY HAT HACKER

Gray hat hackers occupy a unique position between black hat and white hat hackers. They possess the capability to infiltrate systems without authorization to assess their security; however, they refrain from engaging in theft or causing harm to the systems. Typically, they inform the system's administrator of their findings. Despite their intentions, their actions are considered illegal since they conduct security tests without explicit permission. Consequently, gray hat hacking exists in a legal gray area, where it can be deemed lawful in some instances and unlawful in others.Other Types of Hackers are show in Table

Red Hat	A blend of black and white hat, often targeting sensitive information like government data.	Targeting high-security systems, potentially for ethical or unethical purposes.	Advanced hacking skills, targeting government agencies and sensitive data.
Blue Hat	External security testers used by companies (like Microsoft) before product launches.	Bug testing and vulnerability discovery before release.	Security expertise, focused on finding and fixing vulnerabilities.
Elite	Highly skilled hackers recognized for their expertise and discovery of new exploits.	Achieving recognition within the hacking community through advanced skills.	Deep technical knowledge, discovering and sharing zero-day exploits.
Script Kiddie	Non-expert hackers using pre-made tools without deep understanding.	Often motivated by notoriety or disruption, lacking technical depth.	Using readily available scripts and tools, limited technical understanding.
Neophyte (n00b/Green Hat)	New to hacking, with limited knowledge and experience.	Learning the basics of hacking and technology.	Minimal technical skills, in the early stages of learning.
Hacktivist	Hackers using their skills to promote social, ideological, religious, or political messages.	Promoting specific causes through online actions.	Varied technical skills, often using website defacement or DDoS attacks.
Phreaker	Hackers targeting telecommunications networks.	Exploiting telephone systems for unauthorized access or free calls.	Specialized knowledge of telecommunications systems and protocols.
State/Nation-Sponsored	Government-employed hackers conducting cyber operations for national interests.	Espionage, cyber warfare, national security.	Highly skilled, access to significant resources and advanced tools.
alicious Insider/Whistleblower	Employees or insiders with malicious intent or knowledge of illegal activities.	Personal gain, revenge, or exposing wrongdoing.	Insider knowledge of systems and vulnerabilities, potential for blackmail.

Table 3: Other Types of Hackers are show in Table

WHITE HACK HACER VS BLACK HAT HACKER

When people think of hacking, they may picture a shady character crouched over a keyboard, breaking into systems and taking data. Not all hackers, though, are same. White hat hackers, sometimes referred to as ethical hackers or security specialists, apply their expertise for the greater benefit. Working within the bounds of the law, they find weaknesses in networks and computer systems to assist corporations in fortifying their defenses against possible cyberattacks. White hat hackers are also known as sneakers. These people are well-versed in a variety of programming languages and make moral use of their knowledge.

On the other hand, there are also black hat hackers who operate outside of the law. They maliciously exploit system vulnerabilities to gain unauthorized access or cause damage for personal gain. These individuals may commit acts such as data theft, identity fraud, and malware distribution.

While both groups have equal technical skills in hacking tactics, their objectives differ significantly. White Hats want to safeguard enterprises by detecting vulnerabilities before they are exploited by thieves, whereas Black Hats seek personal gain at whatever cost.

IMPORTANCE OF WHITE HAT HACKER

In today's networked world, every organization must ensure that it is adequately protected against all intrusions. All the organization network must be secure with some technique like Firewall and Proxies. For internal system some antivirus software would be use but form outside attack there must be an anti-hacker available for an organization that they check the entire network for variabilities and weakness in the system and must inform them accordingly and this will be done by ethical hacker / White hat hacker tests their defenses in a series of tests to ensure that a real attack can never occur.[12]

White hat hacking is essential for securing critical information systems in our computer-driven world. Although it presents challenges, when utilized effectively, it has the ability to significantly improve information security. Individual hackers' morality and ethics play a crucial role in their success.

White hat hackers are used by corporations, government agencies, and the military to protect and secure sensitive information. To achieve security, it's important to identify and remedy vulnerabilities. Security requires proactive planning to ensure safety and avoid harm.[11]

Identifying and mitigating risks and vulnerabilities before they are exploited by adversaries is critical for information security. If you don't plan ahead, opponents will take advantage of your shortcomings.

As we understand the importance of security and the potential benefits of using white hat hackers, there will be an ongoing battle between newly trained white hat hackers and their competitors in the coming years.

BENEFITS OF ETHICAL HACKING

Ethical hacking provides numerous significant advantages [14]

- **Mitigation of hacking attempts:** By actively uncovering vulnerabilities, organizations can strengthen their security measures and discourage potential intruders.
- **System robustness:** Ethical hackers contribute to the development of resilient systems that are capable of resisting unauthorized access attempts.
- **Financial protection:** They play a vital role in safeguarding banking and financial institutions, ensuring the integrity and security of sensitive data.
- **Detection of vulnerabilities:** Ethical hackers identify and rectify weaknesses in computer systems or networks prior to their exploitation by malicious actors.

METHODOLOGIES OF ETHICAL HACKING

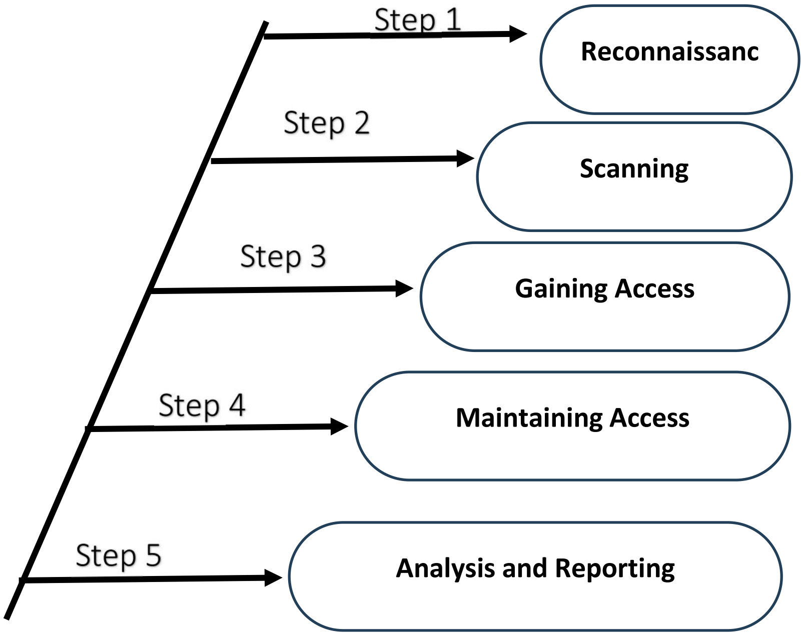

Figure 2: Other Types of Hackers are show in Table

TOOLS FOR ETHICAL HACKING [13]

Tool	Description
OWASP Zed Attack Proxy	A free tool to scan web applications for security issues.
Netsparker	Finds problems like SQL Injection and XSS in web apps automatically.
Acunetix	Automatically tests web apps, including HTML5 and JavaScript
Intruder	An automated tool for finding security flaws in IT systems.
Intruder	An automated tool for finding security flaws in IT systems.
Indusface	Combines manual and automated scanning to find security issues.
SolarWinds Intrusion Detection Software	Monitors for threats in real-time.
W3af	A platform with plugins to find web app vulnerabilities.
Metasploit	Finds software vulnerabilities and helps to exploit them.
Nmap	Maps networks and finds security issues.
OpenVAS	Detects vulnerabilities in host computers/servers.
OpenVAS	Detects vulnerabilities in host computers/servers.
Iron WASP	Used for testing web application vulnerabilities.
Nikto	Scans servers and performs security tests.
Nikto	Scans servers and performs security tests.
SQLMap	Detects SQL-based vulnerabilities.

SQLNinja	Targets web apps using MS SQL Server.
Wapiti	Finds security flaws in web applications.
Ettercap	Comprehensive tool for security testing.
Burpsuite	Intercepts traffic, scans, and crawls web applications.
Arachni	Ruby-based tool for testing web application security.

Table 4: TOOLS FOR ETHICAL HACKING

CONCLUSION

Hacking may be Define as Ethical of unethical or may b define as legal or illegal. This non ending battle of comparison between legal or illegal or white hat Hacker and black hat hacker is a long war, which does not seem to have an end. Ethical hackers play a key role in keeping organizations safe from new and changing threats. They find and fix weaknesses before Black hat hackers can take advantage of them. This review looks at different parts of ethical hacking, including how it has changed over time, the methods used, how it's applied in testing for weak spots, and its overall effect on making organizations more secure. Essentially, ethical hacking is about using hacking skills for good, to find and fix security issues. This helps organizations stay safe from potential attacks. Furthermore, in this study also explain the difference between Black hat Hacker and white hat hacker also focus the way and tools used by these hackers one for gaining the access for his own satisfaction or to destroyed the system or stealing the money from organizations while other is used the same tools for Securing the organization system from this outside attack. List of prominent attack also discuss in this paper for better understanding along with major types of hackers exists in this digital word.

REFERENCES

[1]. D. Raghuvanshi, “INTRODUCTION TO CYBER SECURITY,” 2019. [Online]. Available: http://www.ijeast.com

[2]. A. Singh and G. Kumar, “A Research Paper on Cyber Security,” 2024. [Online]. Available: www.ijrpr.com

[3]. Z. Hussain Butt and F. Nasir, “Ethical Hacking and its role in Cybersecurity Ethical Hacking and its role in Cybersecurity: A Comprehensive Review”, doi: 10.48550/arXiv.2408.16033.

[4]. J. M. Biju, N. Gopal, and A. J. Prakash, “CYBER ATTACKS AND ITS DIFFERENT TYPES,” *International Research Journal of Engineering and Technology*, 2008, [Online]. Available: www.irjet.net

[5]. A. Bendovschi, “Cyber-Attacks – Trends, Patterns and Security Countermeasures,” *Procedia Economics and Finance*, vol. 28, pp. 24–31, 2015, doi: 10.1016/s2212-5671(15)01077-1.

[6]. R. Alabdan, “Phishing attacks survey: Types, vectors, and technical approaches,” *Future Internet*, vol. 12, no. 10. MDPI AG, pp. 1–39, Oct. 01, 2020. doi: 10.3390/fi12100168.

[7]. N. Saud Al-Musib, F. Mohammad Al-Serhani, M. Humayun, and N. Z. Jhanjhi, “Business email compromise (BEC) attacks,” in *Materials Today: Proceedings*, Elsevier Ltd, 2021, pp. 497–503. doi: 10.1016/j.matpr.2021.03.647.

[8]. T. Reddy Kukutla and K. Tejonath Reddy, “A Deep Dive into DNS Spoofing and Security Measures.” [Online]. Available: www.example.com,

[9]. T. Mao, S. Che, and W. Deng, “Research on the Hidden Technology of Troy Trojan-Horse,” 2017.

[10]. S. Sinha and Dr. Y. Arora, “ETHICAL HACKING: THE STORY OF A WHITE HAT HACKER,” *International Journal of Innovative Research in Computer Science & Technology*, vol. 8, no. 3, May 2020, doi: 10.21276/ijircst.2020.8.3.17.

[11]. S. Nanda, “World of White Hat Hackers,” 2019, [Online]. Available: http://www.ijser.org

[12]. V. Kumar, R. K. Chawda, and B. Student, “How Ethical Hackers Play an Important Role for any Organization.?,” 2020. [Online]. Available: www.jetir.org

[13]. “The Importance of Ethical Hacking Tools and Techniques in Software Development Life Cycle,” *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 10, no. 3, pp. 2042–2049, Jun. 2021, doi: 10.30534/ijatcse/2021/791032021.

[14]. B. Sahare, A. Naik, and S. Khandey, “Study Of Ethical Hacking,” *International Journal of Computer Science Trends and Technology*, vol. 2, [Online]. Available: www.ijcstjournal.org