iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** IV **Month of publication:** April 2024

DOI: https://doi.org/10.22214/ijraset.2024.60506

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

Ethical Hacking and Penetration Testing

Tarandeep Singh[1], Akshat Bajpai[2], Samiksha Shukla[3]
[1.2] *Student,* [3]*Assistant Professor, Information Technology, Government Engineering College, Bilaspur*

Abstract: ***Ethical hacking and penetration testing are crucial components of modern cyber security, aiming to identify and rectify security vulnerabilities in computer systems and networks. The huge number of inventions is constantly expanding. Information is getting doubled in less than a year. The advancement of technology has played an important role in our lives. In this era, the most important concern is computer security for companies and organizations. Unfortunately, the data we share over the internet is not secure in any way. Cyberattacks are getting complex and it is hard to detect them. This research paper provides a comprehensive analysis of ethical hacking and penetration testing, discussing their principles, methodologies, tools, legal aspects, and real-world applications.***

Keywords*: Ethical hacking, penetration testing, cyber security, white hat hacking, vulnerability assessment, legal framework, tools and techniques.*

I. INTRODUCTION

In today's connected world, cybersecurity is a pressing concern for organizations of all industries and sizes. The increasing frequency and sophistication of cyber attacks highlights the need for effective security measures to protect sensitive information and ensure the integrity and availability of digital assets. Ethical hacking and penetration testing have become important practices in cybersecurity, providing effective techniques to detect and mitigate vulnerabilities before malicious actors can exploit them.The requirement to protect dominant data of the common people should be communicated with the correct technology. Because of the smartness of hackers, ethical hacking arose as the latest and innovative computer technology [1].

An authorized individual or group seeking to obtain access to a computer, network, or application with the intention of finding and fixing security vulnerabilities is known as ethical hacking, or white hat hacking. This strategy makes sure that hacking operations are carried out properly and responsibly by adhering to the legal, consent, confidentiality, integrity, and availability criteria. By locating weaknesses and putting in place suitable security measures to lower the risk, ethical hacking aims to strengthen organizational security. The term "ethical hacking" refers to hacking that is accomplished by an organization or someone to identify potential future security risks on a computer or device. The business or organization has given them permission to hack its systems in order to maintain security. Hacking ethically entails responsibilities. [2].

II. ETHICAL HACKING

The authorized practice of trying to obtain illegal access to a computer system, program, or data in order to find security weaknesses is called ethical hacking, sometimes referred to as white hat hacking. Principles like availability, secrecy, honesty, lawfulness, and authority serve as its compass. The ethical hacker looks for bugs that a cracker could target by scanning ports, webpages, and other online spaces. Once a device's flaws are identified, conducting an attack becomes simple. A user must understand how a hacker, or cracker, can access his network in order to stay safe in today's internet-driven environment [3]. Learning the principles of hacking and using them to safeguard organizations or systems for worthy causes is known as ethical hacking.

A. Phases of Ethical Hacking

Ethical hackers undertake several steps of the ethical hacking methodology to find such vulnerabilities. These steps of hacking include: Reconnaissance, Scanning, Gaining Access, Maintaining Access, and Clearing Track. While not every hacker follows these steps in sequential order, they offer a systematic approach that yields better results.

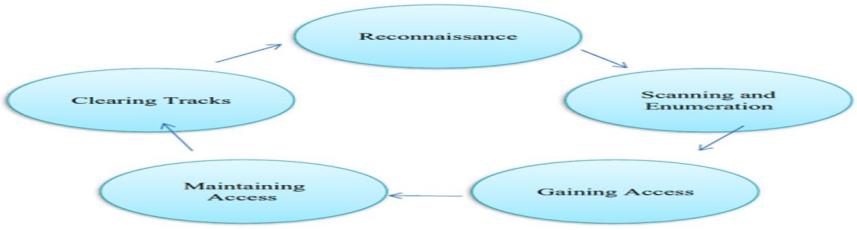


Figure 1 Ethical Hacking Steps

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

Reconnaissance: Before performing any penetration tests, hackers footprint the system and gather as much information as possible. Reconnaissance is a preparatory phase where the hacker documents the organization's request, finds the system's valuable configuration and login information and probes the networks. This information is crucial to performing the attacks and includes:

- Naming conventions
- Services on the network
- Servers handling workloads in the network
- IP Addresses
- Names and Login credentials of users connected to the network
- The physical location of the target machine

1) *Scanning*: During this phase, the machine and network vulnerabilities are tested by the ethical hacker in order to find possible points of attack. This entails employing automated scanning tools to compile data on all devices, users, and services on the network. Usually, penetration testing involves three different kinds of scans:

a) *Network Mapping*: This entails figuring out the host network's topology, including servers, routers, firewalls, and host information. White hat hackers can plan and visualize the subsequent stages of the ethical hacking process once it has been planned out.

b) *Scanning*: The ethical hacker tests the system and network vulnerabilities during this phase to identify potential points of attack. In order to gather information on all devices, users, and services on the network, automated scanning technologies must be used. Typically, there are three types of scans used in penetration testing:

c) *Network mapping*: This comprises determining the topology of the host network, encompassing host information, servers, routers, and firewalls. Once the ethical hacking method is mapped out, white hat hackers may plan and envision the next steps.

- SNMP Sweepers
- Ping sweeps
- Network mappers
- Vulnerability scanners

2) *Acquiring Access*: Following the first and second hacking phases, ethical hackers try to find ways to exploit vulnerabilities in order to obtain administrator access. The third stage entails trying to physically use a linked machine or transfer a malicious payload to the program via the network, a nearby subnetwork, or both. Hackers usually simulate attempted illegal access using a variety of hacking tools and tactics, such as:

- Buffer overflows
- Phishing
- Injection Attacks
- XML External Entity Attacks
- Using components with known vulnerabilities

If the attacks are successful, the hacker has control of the whole or part of the system and may simulate further attacks such as data breaches and Distributed Denial of Service (DDoS).

3) *Preserving Access*: In the fourth stage of ethical hacking, procedures are implemented to guarantee that the hacker will be able to access the program in the future. A white-hat hacker persistently probes the system for new weaknesses and increases privileges to see how much power an attacker may have after gaining security clearance. A backdoor installed for future access and the removal of attack evidence are two more ways that some attackers could attempt to conceal their identity.

4) *Eliminating Traces*: Hackers carry out operations that remove any indications of their activities in order to prevent any proof linking them to malicious conduct. Among them are:

- Uninstalling scripts/applications used to carry out attacks
- Modifying registry values
- Clearing logs
- Deleting folders created during the attack

For those hackers looking to maintain undetected access, they tend to hide their identity using techniques such as:

- Tunneling
- Stenography

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

III. PENETRATION TESTING

The process of examining a computer system, network, or online application to identify security flaws that an attacker could exploit is called penetration testing, or pen testing. Penetration testing is used to find security flaws and evaluate a system or network's security posture. Network penetration testing, web application penetration testing, and wireless network penetration testing are just a few of the several kinds of penetration testing. A methodical technique is used in penetration testing, which includes post-exploitation, vulnerability analysis, exploitation, reconnaissance, scanning, and enumeration. Penetration testing involves simulating a cyberattack on your device to check for any security flaws. Penetration testing is typically used to improve an internet mileage firewall in the context of internet mileage security.

A. Penetration Testing Stages

The pen testing process can be broken down into five stages:

1) *Planning and reconnaissance:* To begin,
- define the objectives and scope of the test, as well as the systems to be tested and the testing techniques to be employed.
- Compiling intelligence (such as mail servers, network and domain names) to gain a deeper understanding of a target's operation and possible weaknesses.

2) *Scanning*: The following action is to ascertain the target application's reaction to different intrusion attempts. Usually, this is accomplished with:
- Static analysis: Examining the code of an application to make an educated guess about how it will operate in real time. With just one pass, these tools are able to scan the entire code.
- Dynamic analysis: Examining the code of an application while it is in operation. This scanning method is more useful because it gives you a real-time image of the application's performance.

3) *Gaining Access:*In this phase, vulnerabilities in a target are found using web application assaults including SQL injection, cross-site scripting, and backdoors. In order to determine the harm that these vulnerabilities can do, testers then attempt to exploit them, usually by gaining more authority, stealing data, intercepting traffic, etc.

4) *Maintaining access:* The objective of this phase is to determine whether the exploitable vulnerability can be leveraged to establish a long-term presence in the compromised system—long enough for a malevolent actor to obtain comprehensive access. The goal is to mimic sophisticated persistent attacks, which can steal the most sensitive data from an organization by staying in a system for months at a time.

5) *Analysis:* The results of the penetration test are then compiled into a report detailing:
- Specific vulnerabilities that were exploited
- Sensitive data that was accessed
- The amount of time the pen tester was able to remain in the system undetected

B. Penetration testing methods

1) *External testing*: External penetration tests focus on a business's online assets, such as the web application itself, the website, email addresses, and domain name servers (DNS). Getting access and extracting useful data is the aim.

2) *Internal testing*: An attack by a malevolent insider is simulated by a tester who has access to an application that is protected by a firewall. It's not always the same as modeling a renegade employee. An employee whose credentials were compromised by phishing is a typical place to start.

3) *Blind testing:* In a blind test, the tester is merely provided with the name of the targeted organization. This provides security professionals with an instantaneous view of how an actual application assault may take place.

4) *Double-blind testing:* In a double-blind test, the security staff is not aware of the simulated attack beforehand. They won't have time to strengthen their defenses before an attempted breach, much like in the real world.

5) *Targeted testing*: In this case, the security staff and the tester collaborate and communicate with one another about their whereabouts. This is an excellent training exercise that gives a security team instant feedback from the perspective of a hacker.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

IV. LEGAL AND ETHICAL ISSUES

The legal framework governing cybersecurity procedures must be followed when conducting penetration tests and ethical hacking. These techniques are governed by laws such as the General Data Protection Regulation (GDPR) in the European Union and the Computer Fraud and Abuse Act in the United States. Getting the right authorization, protecting privacy, getting informed consent, and minimizing harm are all ethical considerations. Understanding and abiding by the moral and legal guidelines guiding their work is crucial for ethical hackers and penetration testers.

A. Legal Concerns

A tester's client may have the following problems as a result of their relationship:

- Since his client is unaware of the tester, why should he be granted access to critical information?
- Who will assume responsibility for the lost security guarantee?
- The client may blame for the loss of data or confidentiality to tester

PENETRATION TESTING- It is crucial to obtain written consent for penetration testing, even for internal testing conducted by inside staff, as it can impact system performance and raise concerns regarding confidentiality and integrity. Before testing begins, a written agreement should be made between the tester and the company, organization, or individual to address all concerns related to data security, disclosure, etc.

Before beginning any testing, a statement of purpose should be written and duly signed by both parties. The job's scope and what you might and might not be doing when conducting vulnerability checks should be made very clear.

For the tester, it is important to know who owns the business or systems which are being requested to work on, and the infrastructure between testing systems and their targets that may be potentially affected by pen testing.

Each party benefits from a formal agreement. Keep in mind that rules vary from nation to nation, so familiarize yourself with the restrictions in the one you live in. Sign a contract only after taking the relevant laws into account.

1) Legal Structure:

a) Computer Fraud and Abuse Act (CFAA): This federal statute in the United States deals with illegal access to computer networks and systems.

b) General Data Protection Regulation (GDPR): This EU regulation safeguards people's personal information and their right to privacy.

c) Additional Laws and Regulations: Depending on the jurisdiction and type of activity, a number of additional laws and regulations may be applicable.

B. Moral Concerns

The possibility of harming or damaging systems and networks is one of the main ethical issues with hacking and penetration testing. It's crucial that you limit the use of your abilities and expertise to appropriate uses, such as assisting businesses in locating and fixing system weaknesses. The target organization's express consent or ethical and legal channels, including bug bounty programs, may be used for this.

The need to uphold confidentiality and safeguard sensitive data presents another ethical dilemma. As a penetration tester or hacker, you might come across private information that, in the wrong hands, could be harmful. Strict secrecy must be upheld, and specified procedures must be followed while handling sensitive data.

Finally, it's crucial to maintain ethical standards when it comes to the use of tools and techniques. This includes respecting the privacy of individuals and avoiding the use of illegal or unethical tools and techniques, such as social engineering.

1) Moral Points to Remember:

a) Getting Appropriate Authorization: Before doing any testing, penetration testers and ethical hackers need to have clear permission from the company.

b) Respecting Privacy: It's critical to uphold people's right to privacy and to keep any private information discovered during testing private.

c) Reducing Damage: It is important for penetration testers and ethical hackers to take precautions against any potential harm that can arise from their work.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue IV Apr 2024- Available at www.ijraset.com

V. TYPES OF CYBER HACKER

1) *White-Hat:* A celebrity who hacks into security systems with non-mischievous intent is known as a "white-hat hacker," or "ethical hacker." Most White-Hat Hackers Are Safety Experts Who Frequently Collaborate With An Organization To Identify & Improve Security Vulnerabilities Lawfully.
2) *Black-Hat:* The so-called "Black-Hat" hackers, sometimes known as "Crackers," are celebrities who hack without authorization and with malicious intent. Hackers often carry out a range of cybercrimes, including credit card fraud, identity theft, and piracy, in an effort to demonstrate their hacking prowess. An individual with in-depth computer knowledge who aims to violate or circumvent internet security is known as a "black hat hacker" [4].
3) *Grey-Hat*: A "grey-hat" hacker is someone who possesses both black and white hat characteristics, as suggested by the color. For instance, some grey-hat hackers will roam the internet looking for compromised systems; like white-hat hackers, the targeted company will be aware of any vulnerabilities and would take action to fix them. However, unlike grey-hat hackers, black-hat hackers will hack without authorization.
4) *Blue-Hat:* Before a program is released, independent computer security specialists are hired to check it for vulnerabilities and identify weak points that can be fixed. Additionally, Blue Hat Participates in Microsoft's Annual Security Conference, Which Enables Open Communication Between Microsoft Engineers and Hackers. Blue Hat Hackers Are Individuals Who Test Computer Security Without Being Employed By A Consulting Firm .
5) *Hacker with Elite Status:* These Hackers Are Known To Be The "Greatest In The Industry" & Are Acclaimed As Innovators & Masters. Elite hackers used a language they invented called "LeetsPeak" to hide their pages from search engines. A language that substituted other similar letters or numerical similarity for a few letters in a word. The term "hacker" is frequently used to characterize someone who secretly obtains access to systems and networks in order to profit from them. Nonetheless, some people engage in the creative art of hacking because the tests they take provide them with a certain level of excitement [6].

VI. TOOLS AND TECHNIQUES

To find and take advantage of vulnerabilities, penetration testing and ethical hacking employ a variety of instruments and methods.The top ethical hacking instruments used by contemporary security professionals. A security investigation can benefit from these technologies. Nmap, Metasploit, Wireshark, Nessus, and Burp Suite are examples of common tools. Social engineering, network scanning, vulnerability scanning, and password cracking are some of the methods employed.

A. *Equipment for Penetration Testing and Ethical Hacking:*

1) *Nmap (Network Mapper)*: Nmap is an effective tool for network scanning that can be used to find hosts and services on a network, as well as open ports and security flaws.
2) *Metasploit Framework:* This penetration testing tool enables testers to evaluate security defenses, create custom exploits, and take advantage of known flaws in a system.
3) *Wireshark:* This network protocol analyzer aids testers in locating and resolving network problems and security flaws by capturing and analyzing network data in real-time.
4) *Nessus*: Nessus is a vulnerability scanner that finds security flaws, incorrect setups, and noncompliance problems in a network while offering thorough reports and remedy suggestions.
5) *Burp Suite: Burp Suit* is a web application security testing tool that assists testers in locating web application security flaws like SQL injection, cross-site request forgery (CSRF), and cross-site scripting (XSS)
6) *Cain & Abel:* Cain & Abel is a Microsoft Operating Systems password recovery program. It facilitates the simple recovery of a variety of password types. A helpful resource for security consultants, qualified penetration testers, and everyone else planning for ethical reasons.
7) *Ettercap:* Ettercap stands for Ethernet Capture. It is a network security tool for Man-in-the-Middle attacks. It features sniffing of live connections, content filtering on the fly and many other interesting tricks.

B. *Methods for Penetration Testing and Ethical Hacking:*

1) *Social Engineering:* This is a tactic used to coerce people into disclosing private information or taking activities that jeopardize security.
2) *Network Scanning:* This technique looks for open ports, active hosts, and services that are using those ports in order to find possible vulnerabilities.

3) *Vulnerability Scanning:* This process looks for security flaws, known vulnerabilities, and misconfigurations on a system or network that an attacker could exploit.
4) *Password Cracking:* This technique allows testers to evaluate the strength of password rules and procedures by utilizing tools and techniques to guess or crack passwords.
5) *Packet Sniffing:* To monitor and troubleshoot network activities, packet sniffing entails capturing and analyzing network traffic.

VII. REAL-WORLD APPLICATIONS

The real-world applications of ethical hacking and penetration testing.

A. *The Equifax Data Breach*

The Equifax data breach in 2017 is one of the most significant data breaches in history. Equifax is one of the largest consumer credit reporting agencies in the United States. The breach exposed the personal information of 143 million individuals, including their names, social security numbers, birthdates, and addresses.

Equifax hired a third-party vendor to conduct a penetration test on its systems. However, the vendor failed to identify a critical vulnerability in Equifax's web application framework, Apache Struts. This vulnerability allowed attackers to gain access to the company's sensitive data.

If Equifax had conducted a thorough penetration test, this vulnerability would have been identified and remediated before the breach occurred. As a result, Equifax paid a hefty price, including paying out $700 million in fines and settlements.

B. *The Canadian Government Cybersecurity Breach*

In 2019, the Canadian government experienced a cybersecurity breach that compromised the personal information of 9,041 individuals. The breach was caused by a vulnerability in the government's online portal for job seekers.

The Canadian government hired a team of experts to conduct a penetration test on its systems. The test identified several vulnerabilities that could have been exploited by attackers to gain access to the government's sensitive data.

The penetration test allowed the Canadian government to identify and address these vulnerabilities before any further attacks could occur. It also helped the government improve its cybersecurity posture and prepare for any future attacks.

C. *Ukrainian government and banking sector DDoS*

On February 15, 2022, the web portal of Ukraine’s defence ministry and the banking and terminal services at several large state-owned lenders were downed in the largest DDoS attacks to hit the country to date. The Ukrainian government publicly attributed the incident to Moscow. The Kremlin has denied involvement in the operation, which hit Ukraine at a time when the country is bracing itself for a possible invasion from Russian forces.

D. *Zloader banking malware:*

Since November 2021, the banking trojan Zloader has been exploiting Microsoft’s digital signature verification method to inject malicious code into a signed system dynamic link library (DLL). The banking trojan leverages Atera, an enterprise remote monitoring and management application, for initial access to targeted machines, and as of January 2022, the malicious DLL had been downloaded to 2000+ unique victim IPs.

E. *Massive data breach by two former employees at Tesla:*

In May 2023, a German news outlet notified Tesla that they had obtained the company’s confidential information. According to Tesla’s data privacy officer Steven Elentukh, “the investigation revealed that two former Tesla employees misappropriated the information in violation of Tesla’s IT security and data protection policies and shared it with the media outlet.”

VIII. CONCLUSION

In conclusion, ethical hacking and penetration testing are essential practices in modern cybersecurity that help businesses find and fix security holes before malicious hackers may exploit them. Organizations that understand the guiding principles, methods, tools, legal repercussions, and real-world implementations of these activities can strengthen their security posture and protect their critical assets from cyber attacks.

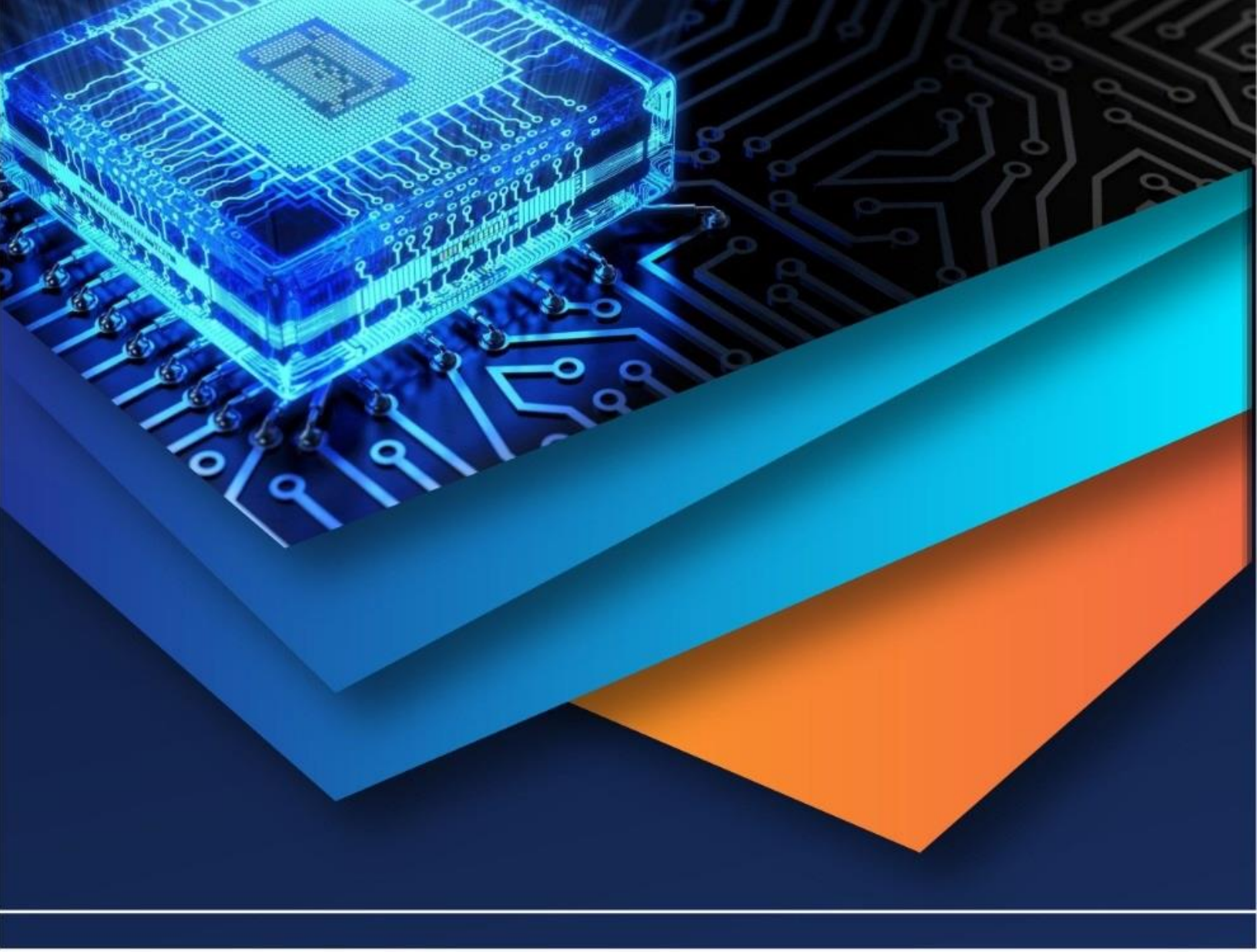
In this research study, we have looked at the foundations, methodologies, available resources, potential legal repercussions, and real-world applications of ethical hacking and penetration testing. We've seen how ethical hackers use their experience to identify and address vulnerabilities in computer systems and networks, while penetration testers imitate intrusions to evaluate the effectiveness of current security measures.

It is clear that ethical hacking and penetration testing are helpful tools for enhancing cybersecurity as well as essential processes for ensuring the availability, integrity, and confidentiality of digital assets. As companies continue to face increasingly sophisticated cyberthreats, there will only be a greater need for skilled ethical hackers and penetration testers.

In conclusion, organizations must prioritize ethical hacking and penetration testing if they hope to effectively protect against online threats. These techniques are critical to modern cybersecurity. By staying current with ethical hacking and penetration testing best practices, organizations may strengthen their security defenses and lower the probability of attacks.

REFERENCES

[1] "Is Ethical Hacking Ethical?," Int. J. Eng. Sci. Technol., 2011.
[2] Haq, Qamar. (2019). /Cyber Security and Analysis of Cyber Crime Laws to Restrict Cyber Crime in Pakistan/. International Journal of Computer Network and Information Security. 11. 62-69. 10.5815/ijcnis.2019.01.06.
[3] B. Sahare, A. Naik, and S. Khandey, "Study of Ethical Hacking," Int. J. Comput. Sci. Trends Technol., 2014.
[4] Norton, "What is the Difference Between Black, White and Grey Hat Hackers?" Emerging Threats, 2019.
[5] S. Tulasi Prasad, "Ethical Hacking and Types of Hackers," Int. J. Emerg. Technol. Comput. Sci. Electron., 2014.
[6] A. Boudreau, L. J. Van't Veer, and M. J. Bissell, "An 'elite hacker': Beast tumors exploit the normal microenvironment program to instruct their progression and biological diversity," Cell Adhesion and Migration. 2012, doi: 10.4161/cam.20880.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY