iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** VI **Month of publication:** June 2022

DOI: https://doi.org/10.22214/ijraset.2022.45047

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 10 Issue VI June 2022- Available at www.ijraset.com

Ethical Hacking Techniques

Shubham Apteka[1], Neharani Baital
Master of Computer Application, Thakur Institute of Management Studies, CareerDevelopment and Research Mumbai University

Abstract: ***The term 'Hacker' was defined to describe experts who utilize their skills to re-develop mainframe systems, increasing their capability and allowing them to multi-task. Nowadays, the term commonly describes skilled programmers who gain unauthorized access into computer systems by exploiting weaknesses or by using bugs, motivated either by malice or mischief. For example, a hacker can produce algorithms to crack passwords, penetrate networks, or even disrupt network services.***
The number one cause of malicious/unethical hacking entails stealing precious records or monetary advantage. However, now no longer all hacking is dreadful. This brings us to another type of hacking: Ethical hacking
Keywords: Ethical Hacking, hacker, authorized, system, hacking, secure, passwords, Access, vulnerabilities

I. INTRODUCTION

Ethical Hacking is a licensed practice of bypassing system security to identify potential data breaches and threats in a network. The company that owns the system or network allows Cyber Security Engineers to perform such exercises in order to test the system's defenses. Thus, unlike malicious hacking, this process is planned, accepted, and especially, legal.
Ethical Hackers intention to analyze the device or community for vulnerable factors that malicious hackers can take advantage of or damage. They bear in mind and accumulate the records to parent out approaches to reinforce the safety of the system/device/network/applications. By doing so, they could enhance the safety footprint in order that it may higher resist assaults, attacks or divert them.
Ethical hackers are hired by the organizations to look into the vulnerabilities of their systems and networks and develop solutions to prevent data breaches. Consider it a high-tech permutation of the old saying "It takes a thief to trap a thief."

A. Key Standards of Ethical Hacking

- *Stay Legal:* Obtain right approval before accessing and performing security assessments.
- *Define the Scope:* Determine the extent of the assessment so that the ethical hacker's work remains lawful and within the approved parameters of the corporation.
- *Report Vulnerabilities:* All vulnerabilities uncovered during the assessment should be reported to the organization.
- *Respect Data Sensitivity:* Depending on the data disclaimer contract, in addition to additional terms and restrictions imposed by the evaluated organization.

II. LITERATURE REVIEW

Ethical hackers use their knowledge to secure and enhance the technology of organizations. They provide an essential service to the organizations by looking for vulnerabilities that can lead to a security threat.
The detected vulnerabilities are reported to the organization by an ethical hacker. Additionally, they provide remediation advice. In many cases, with the organization's permission, the ethical hacker re-tests to assure the vulnerabilities are completely fixed.
Malicious hackers want unlawful access to a resource (the more sensitive, the more preferable) for monetary benefit or personal recognition. Some hostile hackers deface websites or wreck backend systems for amusement, reputational harm, or monetary loss. The methods used and vulnerabilities determined continue to be unreported. They aren't concerned with enhancing the organizations security posture.

III. TYPES OF HACKERS

Hackers can be categorized into different categories such as white hat, black hat, and grey hat, based on their purpose of hacking a system. These words are derived from classic Spaghetti Westerns, in which the bad guy wears a black cowboy hat and the good man wears a white hat.

A. White Hat Hackers

Ethical hackers are another term for white hat hackers. They never intent to harm or damage a device, instead they are trying to discover weaknesses in a computer or a network system as a part of penetration testing and vulnerability assessments. Ethical hacking isn't unlawful and it's one of the demanding jobs available in the IT industry. Many businesses use ethical hackers for penetration testing and vulnerability assessments.

B. Black Hat Hackers

Black Hat hackers also are referred to as **crackers**, those who hack in order to gain unauthorized access to a system and damage its operations or steal delicate data. Their work is always unlawful because of their malicious aim, which includes stealing company data, invading privacy, causing system damage, blocking network connectivity, and so on.

C. Grey Hat Hackers

Grey hat hackers are aggregate of both black hat and white hat hackers. They act without malicious intent but for their fun, they exploit a security weakness in a computer system or network without the owner's permission or consent. Their intent is to carry the weak point to the attention of the owners and getting appreciation or little tip or endowment from the owners**.**

D. Red Hat Hackers

Red hat hackers also are aggregate of both black hat and white hat hackers. They are generally on the extent of hacking government agencies, top-secret information hubs, and usually something that falls under the category of critical records or information.

E. Blue Hat Hackers

A blue hat hacker is someone who works beyond the computer security consulting businesses to evaluate a system before it is released.

They seek for gaps in the system that can be manipulated and try to close them. Microsoft also uses the term **Blue Hat** to represent a sequence of security briefing events.

.

F. Elite Hackers

This is a social position among hackers that refers to the most proficient. Newly discovered exploits will spread among these hackers.

G. Script Kiddie

A script kiddie is a non-professional who breaks into computer systems by using pre-packaged automated tools written by others, usually with little understanding of the underlying concept, subsequently the term Kiddie is used to describe them.

H. Neophyte

A neophyte, "n00b", or "newbie" or "Green Hat Hacker" is a person who's new to hacking or phreaking and has nearly no knowledge, information or experience of the workings of technology and hacking.

I. Hacktivist

A hacktivist is a hacker who makes use of technology to announce a social, ideological, religious, or political message. In general, maximum hacktivism involves website defacement or denial of-service attacks.

IV. ETHICAL HACKING- TOOLS

A. NMAP

Nmap stands for Network Mapper. It is an open source tool that is used for the network discovery and security auditing. It was originally designed to scan massive networks, but it can work even for the single hosts.

Network administrators also dicover it beneficial for tasks such as network inventory, organizing service upgrade schedules, and tracking host or service uptime.

Nmap analyses raw IP packets to detect which hosts are available on the network.–

- What hosts are there on the network,
- What services those hosts are offering,
- What operating systems they are running on,
- What type of firewalls are in use, and other such essentials.

Nmap is compatible with various computer operating systems which includes Windows, Mac OS X, and Linux.

B. Metasploit

Metasploit is one of the most powerful exploit tools. It is a product of Rapid7 and most of its resources can be found at: www.metasploit.com. It is available in two editions: **commercial and free**. It can be used with either a command prompt or a web interface.

You can use Metasploit to conduct the following operations:

- Perform basic penetration testing on small networks.
- Run spot tests to see if vulnerabilities can be exploited.
- Find the network or import scan data.

Exploit modules can be browsed and specific exploits can be launched on hosts.

C. Burp Suit

Burp Suite is a famous platform which is extensively used for performing security testing of web applications. It offers a number of tools that work together to support the whole testing process, from primary mapping and monitoring of an application's attack surface through identifying and exploiting security vulnerabilities.

It is very easy to use and provides the administrators full control to combine advanced manual techniques with automation for efficient testing. It can be easily configured and it also contains features to assist even the maximum experienced testers with their work.

D. Angry IP Scanner

Angry IP scanner is a cross-platform, lightweight IP address and port scanner. It can scan any IP address range. It is free to copy and use anywhere. It employs in order to boost scanning speed multithreaded approach, wherein a different scanning thread is created for each scanned IP address.

It simply pings each IP address to check if it's alive, and then, it resolves its hostname, determines the MAC address, scans ports, etc. The amount of gathered data or information about each host can be saved to TXT, XML, CSV, or IP-Port list files. With the help of plugins, it can gather any information about scanned IPs.

E. Etter Cap

Ettercap stands for Ethernet Capture. It is a network security tool that detects Man-in-the-Middle attacks. It includes live connection sniffing, on-the-fly content screening, and a slew of other intriguing gimmicks. It has built in features for network and host evaluation. Many methods can be dissected both actively and passively.

F. WebInspect

WebInspect is a web application security assessment tool that aids in the identification of known and unknown vulnerabilities in the Web application layer. It may also assist in ensuring that a Web server is correctly setup, as well as attempting common web attacks such as parameter injection, cross-site scripting, directory traversal, and others.

G. LANguard Network Security Scanner

LANguard Network Scanner monitors a network by scanning linked machines and reporting on each node.You can get information about each operating system separately.

It can also track down registry issues and have a report set up in HTML format.You can list the netbios name table, currently logged-on user, and Mac address for each computer.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

H. LC4

LC4 was known as L0phtCrack. It's a password auditing and recovery application. It is used to test the strength of passwords and, in certain cases, to recover lost passwords. Microsoft Windows passwords, by using dictionary, brute-force, and hybrid attacks. It recovers Windows user account passwords to streamline migration of users to another authentication device or to access accounts whose passwords are lost.

I. QualysGuard

QualysGuard is an integrated suite of technologies that may be used to simplify security operations and reduce compliance costs. It automates the whole spectrum of audits, compliance, and protection for IT systems and web applications and delivers essential security intelligence on demand. It comes with a set of tools for monitoring, detecting, and protecting your worldwide network

J. EtherPeek

EtherPeek is a fantastic tool for simplifying network investigation in a multiprotocol heterogeneous network environment. EtherPeek is a lightweight tool (less than 2 MB) tool that may be installed in a matter of minutes.
EtherPeek dynamically sniffs network communication packets. It supports AppleTalk, IP, IP Address Resolution Protocol (ARP), NetWare, TCP, UDP, NetBEUI, and NBT packets by default.

K. Network Stumbler

Network stumbler is a WiFi scanner and monitoring application for Windows. It permits network professionals to detect WLANs. It is extensively used by networking enthusiasts and hackers since it assists in the discovery of non-broadcasting wireless networks.
It can be used to determine whether a network is properly configured, the signal strength or coverage of a network, and to detect interference between one or more wireless networks. It can also be used to connect to non-authorized networks.

L. ToneLoc

ToneLoc stands for Tone Locator. It was a popular war dialling computer program written for MS-DOS in the early 90's. "War dialling" is a technique that involves using a modem to automatically scan a list of phone numbers, typically dialling every number in a local area code. Malicious hackers utilise the generated lists to compromise computer security, such as guessing user passwords or locating modems that could give an entry point into computer or other electronic systems. Security staff can use it to detect unauthorised devices on a company's telephone network.

V. PROCESS OF ETHICAL HACKING

Ethical hacking has a set of different phases. It enables hackers to carry out a well-structured ethical hacking attack. The entire procedure can be divided into six stages, which are as follows:

A. Reconnaissance

Reconnaissance is the stage in which an attacker obtains knowledge about a target through active or passive means. NMAP, Maltego, and Google Dorks are some of the tools commonly utilized in this procedure.

B. Scanning

During this stage, the attacker actively probes a target system or network for weaknesses that can be exploited. Nessus, Nexpose, and NMAP are the tools utilised in this approach.

C. Gaining Access

The vulnerability is discovered during this procedure, and you attempt to exploit it in order to get access to the machine. Metasploit is the major tool utilized in this process.

D. Maintaining Access

It is the method through which a hacker gains access to a system. After getting access, the hacker instals several backdoors in order to enter the system in the future if he requires access to this owned machine. In this approach, Metasploit is the ideal tool.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue VI June 2022- Available at www.ijraset.com

E. Clearing Tracks

This procedure is, in fact, unethical. It is related to the deleting of logs of all activities that occur throughout the hacking process.

F. Reporting

The final step in the ethical hacking procedure is reporting. Here, the Ethical Hacker creates a report containing his findings and the task that was completed, such as the tools used, the success rate, vulnerabilities discovered, and techniques employed.

VI. COMMON HACKING TECHNIQUES

A. Phishing

Phishing is the most common hacking techniques. All of our inboxes and text messaging apps are filled with phishing messages daily. These are messages which are disguised as either as an organization (Amazon, Netflix, etc.) or a person that you trust and will, in maximum cases, tell a story to mislead you into opening an attachment or clicking on a link.

B. Bait and Switch Attack

Using trusted marketing methods such as paid-for advertising on websites, attackers can trick you into visiting malicious sites. When websites sell advertising space, rogue attackers can buy it. The bona fide advertisement can be replaced with a 'bad' link that can be used to download malware, lock up your browser, or compromise your system structures.
Alternatively, the commercial may link to a legitimate website, but it will be programmed to redirect you to a harmful site.

C. Key Logger

A key logger is a small piece of software program that, when downloaded into your computer, will record every keystroke. The key logger will capture every keystroke on the keyboard, every username, id, password and credit card number, etc., exposing all of your data and private information.

D. Denial of Service (DoS\DDoS) Attack

A Denial of Service attack is a hacking methodology designed to flood your web server with a myriad of requests to the point that it overloads the web server resulting in a website crash.
To do this, hackers will use botnets or zombie computers with a single goal: to flood your website with data requests.

E. Click Jacking Attacks

This method tricks you into clicking on something different from what you thought you were clicking. A clickjacking element could be a button on a web page that, when clicked, performs a different function, allowing outsiders to gain control of the machine. The host website may not be aware of the existence of the clickjacking detail.

F. Fake W.A.P.

A hacker can make use of software to impersonate a wireless access point (W.A.P.), which can connect to the 'official' public place W.A.P. which you are using. Once you get connected to the fake W.A.P., a hacker can gain and access your data. To idiot you, the hacker will supply the fake W.A.P an apparent genuine name such as 'T.F. Green Airport Free WiFi.'

G. Cookie Theft

The cookies in our web browsers such as Chrome, Morzilla,Safari, etc, save personal data like browser history, usernames, and passwords for various websites we visit. Hackers will send I.P. (data) packets that pass through your computer, and they can do that if the website you are browsing doesn't have an SSL (Secure Socket Layer) certificate.
Websites that begin with HTTPS:// are secure, whereas sites that start with HTTP:// (no 'S') do not have SSL and are NOT considered as secure.

H. Viruses and Trojans

Viruses or Trojans are malicious software program packages that, when it gets installed on your computer, will send your data to the hacker. They also can lock your files, spread to all the computers linked to your network, and carry out many different unkind actions.

VII. RESEARCH METHODOLOGY

We conducted a survey where we asked few questions to the people about how much they are aware of Ethical Hacking. The results are shown below:

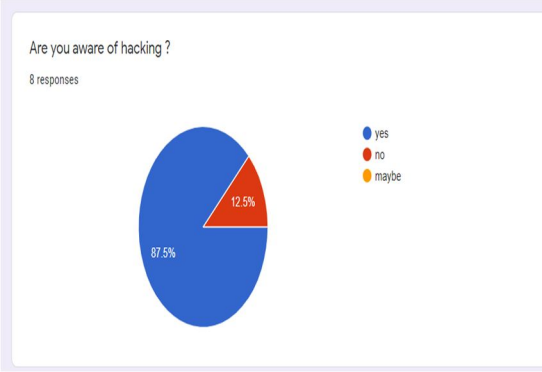


Figure 1

This shows people are aware of the term of hacking.

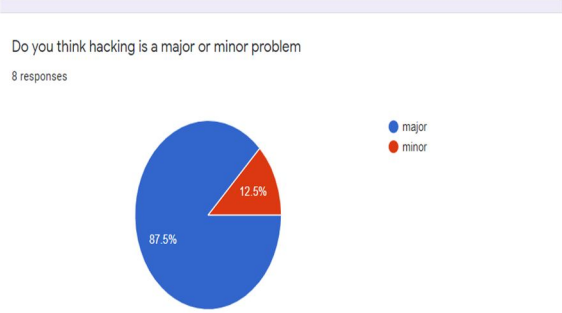


Figure 2

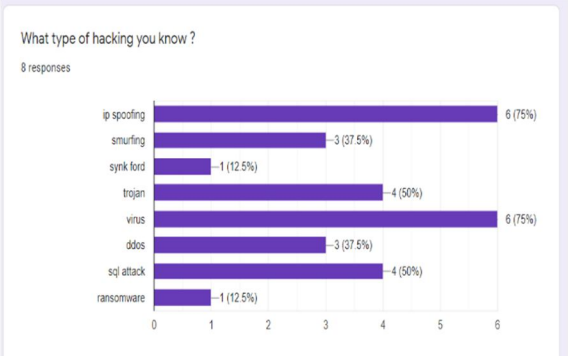


Figure 3

Both the above figure shows that people are having rough knowledge of hacking. But more awareness or knowledge should be spread in order to how to deal with it.

VIII. MEASURES TO BE TAKEN TO PROTECT YOUR SYSTEM FROM HACKERS

A. Install an Anti-spyware Package.

Spyware is a type of software that secretly monitors and gathers personal or corporate data. It is designed to be difficult to detect and delete, and it frequently displays unsolicited adverts or search results that are intended to send you to specific (often malicious) websites.

B. Install Antivirus Software

Antivirus software plays an important part in securing your system by identifying real-time threats and ensuring the safety of your data. Some powerful antivirus systems offer automatic updates, further protecting your machine from new threats that appear on a daily basis. Don't forget to use your antivirus application after you've installed it. To keep your computer virus-free, run or schedule frequent virus scans.

C. Use Virtualization

Not everyone needs to go this path, but expect to be inundated with spyware and viruses if you visit dubious websites. While avoiding hazardous websites is the greatest strategy to avoid browser-derived incursions, virtualization allows you to operate your browser in a virtual environment, such as Parallels or VMware Fusion, that bypasses your operating system to keep it safe.

D. Use Complex Passwords

The most important strategy to prevent network breaches is to use safe passwords. The more secure your passwords, the more difficult it is for a hacker to infiltrate your system.

More secure frequently equates to longer and more complex. Use a password with at least eight characters that includes a mix of numbers, uppercase and lowercase letters, and computer symbols. Hackers have a plethora of tools at their disposal to crack short, simple passwords in minutes.

E. Secure Your Network

Routers are not typically shipped with the maximum security settings enabled. Log in to the router and set a password using a safe, encrypted setup while configuring your network. This keeps intruders from breaking into your network and fiddling with your settings.

F. Use Encryption

Even if hackers acquire access to your network and files, encryption can prevent them from accessing any of your data. You can encrypt your Windows or macOS hard disc with BitLocker (Windows) or FileVault (Mac), encrypt any USB flash drive containing critical information, and encrypt online traffic with a VPN. Only shop on encrypted websites; you can tell by the "https" in the address bar, which is accompanied by a closed-padlock image.

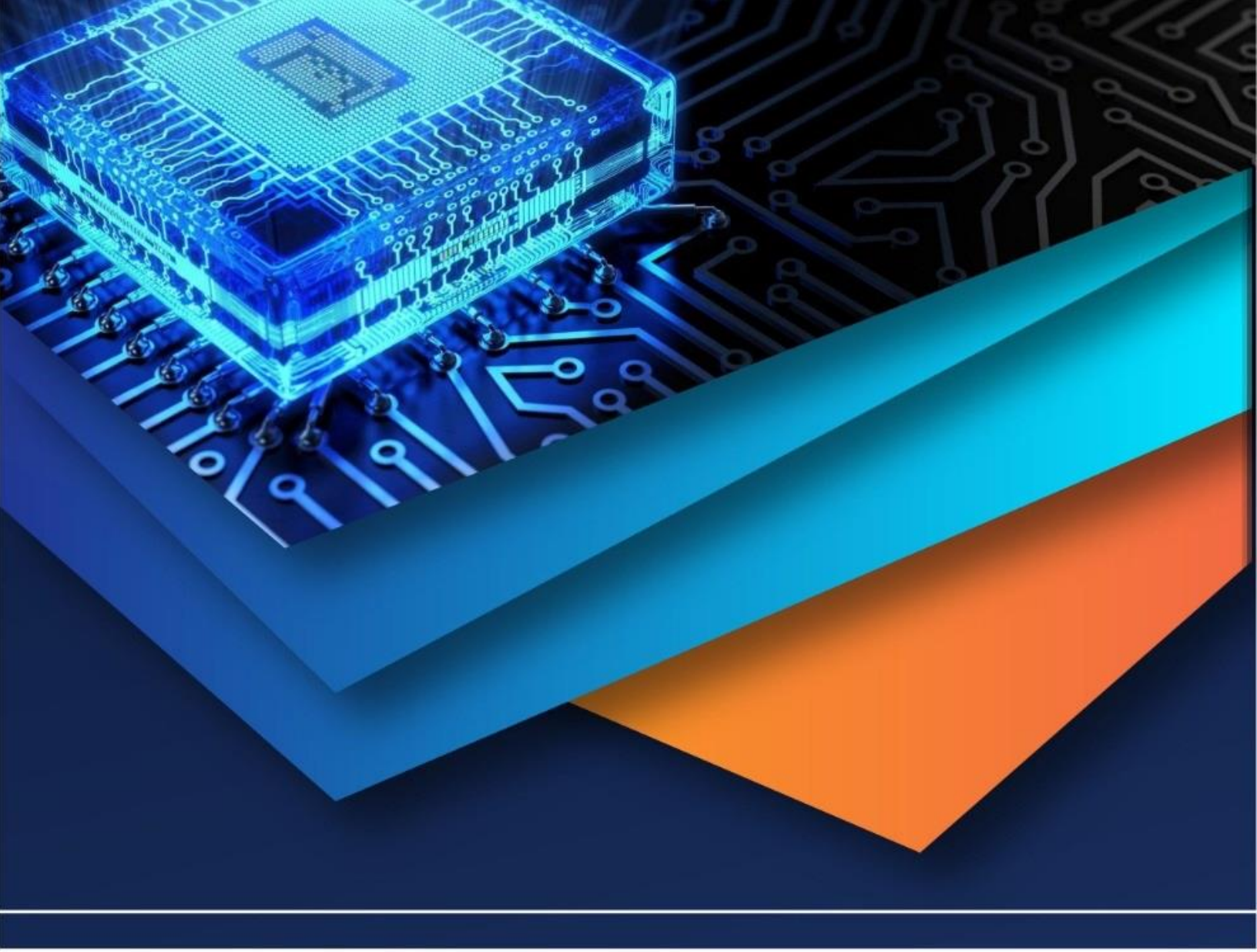
IX. CONCLUSION

Ethical hacking is not a criminal activity and it ought to now no longer be taken into consideration as such. While harmful hacking is a computer crime and a criminal activity, ethical hacking is never a crime. Ethical hacking conforms to industry regulations as well as organizational IT policy.

Malicious hacking should be prevented while ethical hacking which promotes research, innovation, and technological breakthroughs ought to be recommended and allowed.

REFERENCES

[1] Sukhai, N.B. (2004). Hacking and cybercrime. InfoSecCD Proceedings of the 1st annual conference on Information security curriculum development, ACM. pp. 128-132.
[2] Machin, S. and Meghir, C. (2004). Crime and economic incentives. Journal of Human Resources, 39(4), pp.958-979.
[3] Caldwell T. (2011). Ethical hackers: Putting on the white hat. Network Security. pp.10-13. doi: 10.1016/s1353- 4858(11)70075-7
[4] https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_quick_guide.htm
[5] Conrad J. (2012). Seeking help: The important role of ethical hackers. Network Security. 2012(8), pp.5-8. doi:10.1016/s1353- 4858(12)
[6] https://en.kali.tools/?p=107
[7] Elsevier B.V (2002). In argentina, judge ruled that hacking is not a crime, Computer fraud & security, 2002(5), p.20.
[8] Farwell J.P., Rohozinski R. (2011). Stuxnet and the future of cyber war. Survival.
[9] Fehr C., Licalzi C., Oates T. (2016). Computer crimes. The American Criminal Law Review, 53(4)
[10] https://hack4net.github.io/Hacking-Tutorial/



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY