e-ISSN: 2582-5208
International Research Journal of Modernization in Engineering Technology and Science
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
Volume:05/Issue:09/September-2023 Impact Factor- 7.868 www.irjmets.com

CYBERSECURITY IN THE MODERN WORLD: ETHICAL HACKING

Saachi Joshi[*1], **Khushal Chauhan**[*2], **Mayur Ghawate**[*3], **Sejal Kulkarni**[*4]

[*1,2,3,4]Student, Department of Science and Technology, Vishwakarma University, Pune, Maharashtra, India.

DOI : https://www.doi.org/10.56726/IRJMETS44859

ABSTRACT

In this research paper we investigate the topics of ethical hacking and penetration testing in the modern world of cybersecurity. In the current world where cyberattack has become serious issue. Ethical hacking, which can be studied prior and then applied on real world applications and software so that the data cannot be exploited and misuse. By conducting survey and doing research we have found many new tools and technique that are used in ethical hacking.

Keywords: Penetration testing, Ethical Hacking, Cyber Security, Threats, Vulnerability Management.

I. INTRODUCTION

In a generation of digital change where every person and devices are connected to each other, the cybersecurity has become the important aspect of our life and data. With the technology upgrading itself the threats are also increasing day-by day. So, the ethical hacking and penetration testing have become a tool for finding vulnerability and cyber threats. One often thinks that these two terms are synonyms of each other. However, that is not the case.

The main motive behind penetration testing is to find out the vulnerability and report it to the concerning authority before the criminal exploits it. Whereas Ethical hackers study the whole security system of the company. But their work is not limited up to finding vulnerabilities, they also suggest solutions for solving them. In this paper we will also cover what is hacking, types of hackers, how can we protect ourself, tools used for ethical hacking, methods of attack, different phases of hacking, legal implications, prerequisites for becoming ethical hacker, career opportunities. Moreover, we will also mention the new trends such as Bug bounty program, and Hackathons.

II. METHODOLOGY

What is Hacking?

Hacking is a technique which includes compromising computers or devices to gain the access, this access can be authorize or unauthorize depending on the intention of the hackers.

The hackers find loopholes or weakness in the systems or networks to gain entry for the exploitation of data. Many Organizations hire these hackers to find the weakness in their own systems. Some hackers pose as a benefit for a organization where as some hackers pose as a threat. For better understanding let us term them as righteous and malicious hackers.

Righteous hackers- These hackers aim to report the vulnerabilities they found in the system for the protection of organization for example- penetration testers.

Malicious hackers- These hackers exploit the vulnerabilities they found for their own benefit for example-cybercriminals

Types of Hackers-

As mentioned above about righteous and malicious hackers these are also termed technically as:

Hackers come in various types, and their motivations and intentions can vary widely. Here are some of the main types of hackers, along with detailed explanations:

1.White Hat Hackers:

These are the individuals who use their hacking techniques for valid reasons. They are usually appointed by companies or organizations to test and eradicate the vulnerabilities in their systems. These white hat hackers execute vulnerability assessments, penetration testing and review the security policies of the organizations or companies. These hackers are generally driven to safeguard systems from cyber-attacks. These are also called as ethical hackers.

2.Black Hat Hackers:

Black hat hackers are malicious hackers who are involved in illegal work to gain entry in networks and systems. They are mostly involved in activities consisting of stealing personal information, selling them on dark web and ransomware attacks. These hackers are generally related with criminal activities. Black hat hackers are inspired by personal revenge, financial profit or just to cause harm and destruction.

3.Grey Hat Hackers:

These hackers work in between white hat and black hat hackers. They don't have any wrong intent but they don't have proper permissions from the owners to access their systems and networks. Grey hat hackers may find vulnerabilities and notify the affected organization, but they mostly do it without taking permission from the organization.

As they mostly do it without taking permission, they also have to face legal actions from the authorities.

Phases of Ethical Hacking-

There are mostly five different steps which ethical hacker uses to find any vulnerabilities present in the system of any organization. These steps are-

1) Foot Printing-

Foot printing is the very first step which hacker uses. In this process hacker tries to gather all the information of the targeted organizations or victims. This part is also called as information gathering. It can generally be done in two ways first is gathering information available publicly and the second way is by communicating with the selected system. Hackers uses various online tools to gather publicly available information such as WHOIS lookups, this tool helps to find the detailed information about ip address and domain names.

2) Scanning and Enumeration-

After collecting the information from the step one, Hacker moves on to the second step which is Scanning and Enumeration. In this step hacker tries to find out the loopholes or any weaknesses in the system or network through which he can get the entry point. Attackers use tools like network scanners like Wireshark and Nmap to find open ports, services running on those ports, and potential flaws.

This step also includes withdrawing information of the targeted system, for examples user version of the software's, details about the operating systems. This step is very crucial for hacker as critical for identifying vulnerabilities.

3) Gaining Access

This phase is the main objective of the hacker as the actual intrusion starts from this phase Once vulnerabilities or weaknesses are found, the hacker tries to get into the loophole of the system without any permission [Unauthorized Way]. The hacker starts using various methods for getting into the system. This method consists of various techniques like SQL Injection, Bypassing the authentication present in the system, bypassing firewall security, escaping intrusion detection systems. The aim of the hacker is to obtain the proper access of the systems.

4) Maintaining access

Once the hacker successfully gets the access of the system, the main objective is to maintain and control the compromised system for a long period of time. The hacker makes sures that he has continued access to carry out further malicious attacks on the systems. Hacker generally creates the backdoor in the systems which will allow them to re-enter the system again without performing the same process again. To avoid being getting detected hackers continuously monitor the system and network through which they have gained the access.

5) Clearing the tracks

This is the final step a hackers must not forget before leaving the system. That is clearing the tracks. In this final step, hackers should aim to focus on covering their tracks to avoid getting detected by cyber security professionals and system admins. They should generally destroy the proof of their appearance in the systems and all the activities perform by them, by deleting all the log files and history. This is a very important part for avoiding being caught which may cause them future legal problems.

-Tools Used by Ethical Hacker:

Ethical hackers use many different tools and various techniques to find the vulnerabilities in computers, networks, devices and in many other systems. These tools are generally used with the proper permission of the respective owner of the systems or devices to fix security flaws and improve it.

Here are some of the tools that are used-

1)Network Mapper (Nmap)

Nmap helps to identify the running services and open ports of targeted operating system. This tool is one of the most commonly used by hackers. This tool is also used for network scanning and security audits.

2)Wireshark

Wireshark supports wide range of network protocols and it can decrypt the detailed information about packets flags, payloads and headers. Wireshark helps to capture network traffic and inspect it parallelly. This tool helps to capture the information of packets which are sent from source to destination and analyze it for any suspicious or malicious traffic present in the network which can be a threat for the system.

3)John the Ripper

This tool is mostly used for cracking passwords of various file formats. For security audits this tool helps to check the strength of passwords. This tool also supports various methods for password cracking like Brute force Attack and Dictionary Attack.

4)Burp suite

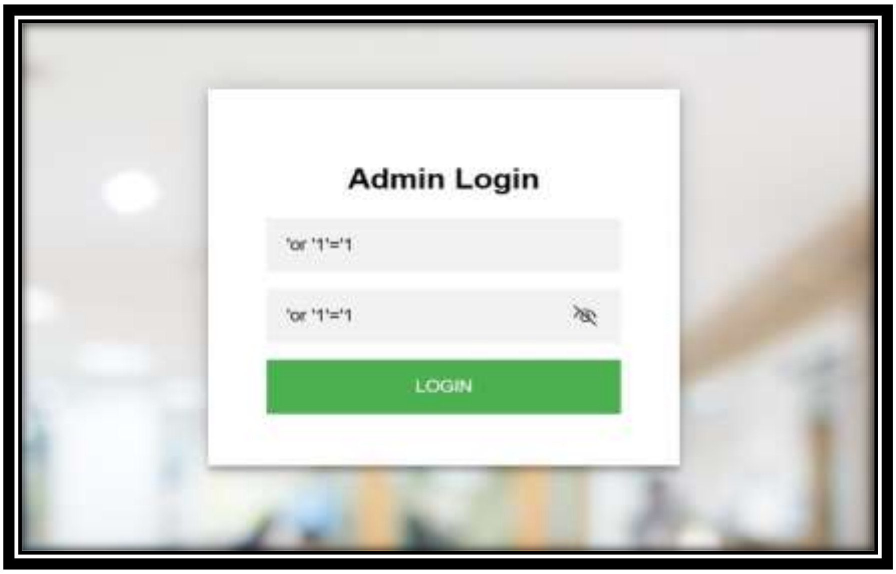
Burp suite is most widely and most used tool by penetration testers around the world.

It intercepts in between the browser and the server while sending any requests. This tool helps us to modify request sent by the browser to the server. This tool helps in identifying many vulnerabilities present in the web application.

-Methods of attack

1)SQL Injection-

SQL Injection is a type of attack that mainly focuses on databases and websites by exploiting vulnerabilities. This attack allows an attacker to modify the SQL queries. Through which we can get access of all databases in which hacker can modify, delete or edit. The hacker searches for a website that is vulnerable to SQL Injection by providing various payload in the input fields of admin login pages. So, if its successful hacker can gain admin access of website. For example, the hacker might input these ' OR '1'='1(as shown in Fig1) in a username or password field, which makes the query true and allows them to log in without correct username or password. Another commonly used payload is '; DELETE FROM users; --, This payload allows hacker to delete any type of data from the user's database.



Admin Login

'or '1'='1

'or '1'='1

Fig 1: SQL INJECTION

2) Man-in-the-Middle (MitM) Attacks:

A Man-in-the-Middle (MitM) attack is a attack where a hacker intercepts and possibly changes the information shared between two users without them knowing or without their permission. In a Man-in-the-Middle attack, the hacker secretly places themselves between the users, which allows them to listen in on the conversation, change it, and even imitate one or both users. The attack process includes initial research to identify potential victims and placing themselves between users. The attacker then infiltrated data, possibly changing it, collecting important information. The exploited data may be misused for the benefit of the hacker.

3) Social Engineering: -

Social Engineering is a manipulation strategy used by hackers to trick users or companies into exposing confidential data, or providing backdoor entry in their systems. It takes disadvantage of human behavior and trusting capability, instead of being dependent on technical weaknesses. There is various type of social engineering attacks that can take entire companies, users, individuals and staff members.

Reverse Social Engineering: In this case, the user contacts the expert (hacker), who impersonates a helpful expert to trick the user into reliving sensitive data.

Phishing: hacker send misleading, messages, emails, or application that appear to be genuine ones to trick receivers into exposing sensitive data like personal data, usernames, passwords, debit card numbers.

Pretexting: The attacker creates a false scenario to obtain sensitive data. This usually involves mimicking someone who is at important position, like an employee, manager, Director and service provider.

4) XSS (Cross Site Scripting):

Cross-Site Scripting (XSS) is commonly found security vulnerability in many websites. That allows hackers to insert infected script into pages of websites which can be viewed by other users. These scripts can change the context of the page it can also steal users' sensitive information. These attack takes place when website doesn't have proper input validations. The hacker has to be proficient in JavaScript to execute cross-site Scripting. The hacker injects this script into the website, such as providing it in an input field, adding it to a URL. or injecting into user's database. When other users access the victims page, their web pages and execute the malicious script, which can steal their sensitive data, cookies, sessions, or other, or any other action performed by the user.

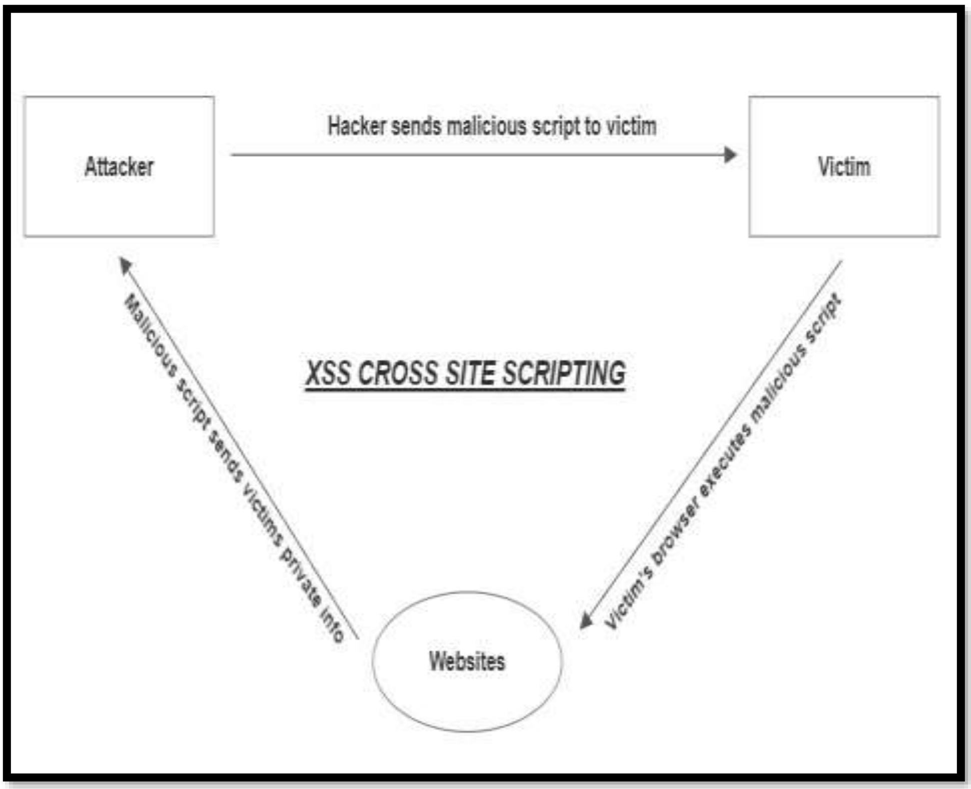

Attacker
Hacker sends malicious script to victim
Victim
XSS CROSS SITE SCRIPTING
Malicious script sends victims private info
Victim's browser executes malicious script
Websites

Fig 2: XSS CROSS SITE SCRIPTING

-How can we protect ourselves-

White hat hackers, also known as ethical hacker are those who are experts in this field to identify and address vulnerabilities in any in any web applications, system and networks, to enhance the security. Here are few ways to safeguard yourself from any malicious activity:

1)Regular Software Updates:

Software updates, also known as security updates or software updates which are given by software team, engineers and organization to fix various problems in a software.

Why are they necessary?

Bug Fixes: Updates also repairs the security-related bugs and flaws or problems that can crash the fastness, performance, or efficient working of the application or software. These faults may lead to data loss, crashing of the application and many other problems.

New Features: Majorly a software team or developers may introduce new features in application which can be included in software updates.

2) Use Unique and Strong Passwords:

One should always change default passwords. As these are often widely found online and can be used by attackers. It is always suggested that one must use different and strong password. These strong passwords should contain alphabets, numbers, and special characters also it should be containing at least 12 to 16 characters long. As these passwords would be difficult to brute force.

If you use the same password for several accounts and one of them gets compromised, it puts all your other accounts at threat.

Using different passwords help to protect our personal information from attackers as our social media accounts contain personal information like name, date of birth, E-mail.

3)Upskill Your knowledge:

Keep yourself updated to the latest threats in the industries. One should not click or visit any unknown websites or link sent by anonyms person. Before downloading any files from any website check the legitimacy of it.

Many securities violation happens due to human mistakes, so basic education about cybersecurity is key. It is also suggested to use VPN (Virtual private network) for safe browsing. Also, Antivirus should be installed in system to defend against any malicious virus or ransomware.

-Legal Implications-

White hat hackers, also called as ethical hackers or penetration testers, these people often get engaged in many cybersecurity activities with owner's permission or permission from the companies to identify and fix security weakness or loopholes present in the systems. To ensure proper legal measures, they must get proper authorization agreements and strictly follow it. They must also handle the sensitive information with care following proper data protection laws.

Penetration testers, usually sign (NDA) non-disclosure agreements with the organizations, before performing any kind of attacks on their systems. They also need to maintain proper record of their activities with transparency with their clients. They should consider obtaining proper legal guidance. They must also follow the country's law which organization is being operated.

Ethical hackers should not share the vulnerabilities publicly which they have found while testing without the permission of the particular organization or company. Before disclosing publicly hackers must give some time to the organization to fix the issue properly in their system.

-Prerequisites for becoming ethical hacker

a) To become an Ethical Hacker Strong Fundamentals in Computer Science and Information Technology is required. They should have strong concepts cleared in networking, computer systems, operating systems and basic programming languages. One wanting to pursue this career must have bachelor's degree in information technology, computer science or an any other similar field.

b) One must also have Technical Skills like Proficiency in programming languages like C, C++, Java, Python or scripting language is which is important for developing the knowledge about the exploits.

c)Familiarity with concepts and working of operating systems like Windows and Linux. Proper knowledge of security tools and techniques, including penetration testing tools, network scanning, and vulnerability assessment.

d)Cybersecurity Knowledge is achieved by strong understanding of different security concepts, methods and principles. One must also study topics such as ethical hacking techniques, cryptography, web application security, and network security.

e) In this field hands on experience are very important part. After gaining the proper knowledge you must practice it on virtual labs to gain the confidence. For better experience and knowledge participate in various programmers like bug bounty, CTF (Capture the Flags) to enhance your skills.

f) Understand yourself with the legal and ethical aspects of hacking. Ethical hackers must always follow the proper guidelines provided by the law. You must dedicate and committed for using your skills for legal purposes only.

g) Ethical hackers must properly communicate their research about the vulnerability clearly to users and companies. Proper verbal and written communication must be done as they are very important for the smooth running of the organization.

-Career Opportunities in Ethical hacking-

There are various opportunities for Penetration tester and ethical hacker which offers a different range of golden opportunities in this ever-evolving field of cybersecurity. Ethical hackers, also called as White hat hacker, Penetration testers or Cybersecurity experts, which play a vital role in defending vulnerabilities of their organization from cyber threats. These experts are masters in recognizing and helps in finding flaws within their website, web applications, network, and computer system to prohibit the cyber-attacks. They use various techniques and tools to perform cyberattacks and evaluate companies' security position. They also provide detailed report and advice to increase security. There are various roles in the field of cybersecurity such as Certified Information system security professional (CISSP), incident responders, Vulnerability assessment and Penetration tester (VAPT), cybersecurity analyst, cybersecurity consultant and Chief information security officer (CISO) these are the positions that one can choose as a career path in field of cybersecurity for the ethical hacking. Ethical hacking also provides many different opportunities in this field. Upgrading your skill is very important aspect in this field like keep updates on new threats in the markets and their solutions. These people should be well certified.

III. RESEARCH AND FINDINGS

One of the main objectives of this research papers is to circulate the understanding of ethical hacking to the world. In this research we found that the people or any organization should be well aware with the techniques used by ethical hacker to keep them safe. This research will contribute to spread general awareness to the public. This paper on ethical hacking can help as educational material for one who is keen for learning this topic in detailed manner. As we all know this is growing and developing field. Where many people can express their knowledge and contribute towards this field. As this paper may highlight all the ongoing and upcoming threats. This Research in ethical hacking generally includes various techniques tools, legal implication, and future scope for ethical hackers.

Below are some of the stats and reports related to cyber security: -

1) According to the 'Cybersecurity Ventures' – Crimes related to security is expected to cost the globe $8 trillion USD in 2023. ………. (1)
2) Other stats we found during research that global cybercrime may damage costs to increase by 15 % annually for the next three years. Target of reaching $10.5 trillion USD per year by 2025…………. (1)
3) According IBM Data breach reports 51% companies are deciding to improve their security. For continuous 13 years United states of America holds the title for highest data breach cost i.e., USD 9.48 Million………… (2)
4) According to the survey conducted by TAC security it reveals that Number of business (71%) reported that their greatest security concern is E-mail Phishing…. (3)
5) According to the survey conducted by TAC security it reveals that that Number of businesses uses many tools to scan their networks is 82%.........(3)

6) The average salary of cybersecurity analyst is $107,517, reported by cyber seek …… (4)
7) In year 2023 pay scale reported that $92,779 is the average salary for penetration tester…… (5)
8) According to the research done by positive technologies penetration tester found out that the number of companies that were using outdated versions of software's are 60% and 85% of companies had critical high risk password policies. …… (6)
9) The Synopsys AST service conducted tests where 78% fell into an OWASP Top 10 risks for the total 30,731 vulnerabilities they discovered…… (7)
10) According to OPSWAT- Web application security survey 2021 claims that 82% companies has concerned about file upload attacks in previous years……. (8)

IV. CONCLUSION

Through this research paper we have explored the world of world of ethical hacking. Observing various facts in this evolving domain. We started our paper by all the fundamentals related to the ethical hacking. We also explained hacking surrounded a large areas of activities like malicious security threat for securities. We also included different Types of hackers which are recognized widely, with efforts ranging from criminal purpose to ethical purpose. Ethical hackers, uses various tools and technique for identifying the vulnerability and exploiting the data. Protecting oneself from cyber threats involves pre awareness of the threat in the industry, Keeping solution ready for the upcoming vulnerabilities. Hacking includes various phases from foot printing to exploitation of information, with proper legal involvement of the organization. Ethical hackers require a great knowledge of this area and should be appropriately certified. Which provides various opportunities in their continually growing domain. In this evolving world of digitalization world, having the knowledge of ethical hacking and cybersecurity is crucial for all the users, and organizations

V. REFERENCES

[1] https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/
[2] IBM Cost of a Data breach report 2023 retrieved from-- https://www.ibm.com/reports/data-breach
[3] https://tacsecurity.com/tac-security-survey-reveals-88-of-businesses-rely-on-manual-processes-to-identify-network-vulnerabilities/
[4] https://www.cyberseek.org/pathway.html
[5] https://www.payscale.com/research/US/Job=Penetration_Tester/Salary
[6] https://www.ptsecurity.com/ww-en/analytics/results-of-pentests-2022/#id10
[7] Software Vulnerability Snapshot by Synopsys Security Testing Services retrieved from-- https://www.synopsys.com/software-integrity/resources/analyst-reports/software-vulnerability-trends/thankyou.html
[8] OPSWAT- Web application security survey 2021-- https://info.opswat.com/web-application-security-report-2021
[9] https://pentest-tools.com/blog/penetration-testing-statistics
[10] 2023 SonicWall Cyber threat Report-- https://www.sonicwall.com/2023-mid-year- cyber-threat-report/